2005-09

An analysis of 802.11b and 802.16 technologies as part of the tactical internet

Swearingin, Brad E.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN ANALYSIS OF IEEE 802.11B AND 802.16 TECHNOLOGIES AS PART OF THE TACTICAL INTERNET

by

Francisco A. Caceres
Brad E. Swearingin

September 2005

Thesis Advisor: Rex Buddenberg
Second Reader: Carl Oros

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: An Analysis of 802.11b and 802.16 Technologies as Part of the Tactical Internet			**5. FUNDING NUMBERS**
6. AUTHOR(S) Caceres, Francisco A and Swearingin, Brad E.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Marine Corps Tactical Systems Support Agency (MCTSSA)			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This research evaluates IEEE 802.11b and 802.16 technologies to examine whether these wireless technologies can integrate into the tactical Internet. In order to establish a baseline, the current Marine Corps' systems architecture is analyzed with emphasis placed on mobile forces at the Regimental level and below. A side-by-side comparison between existing communication assets in the Marine Corps inventory, such as the Enhanced Position Location Reporting System (EPLRS) and Single Channel Ground and Airborne Radio System (SINCGARS), and available 802.11b/16 technologies will evaluate whether existing Command and Control requirements are met, determine the existence and extent of excess capacity, and identify potential adaptations required to implement commercial-off-the-shelf (COTS) technology into a military environment.

The method for side-by-side evaluation will incorporate both COTS products as well as Marine Corps tactical communication devices in laboratory as well as field experimentation. This research captures key performance metrics such as range, power consumption, security, and bandwidth, but remains focused on the needs of the warfighter by evaluating performance of the system in support of Command and Control Compact Edition (C2CE) and Command and Control Personal Computer (C2PC) applications.

14. SUBJECT TERMS 802.11b, Wi-Fi, SecNet-11, OLSR, MANET, MESH, C2PC, C2CE, 802.16, WIMAX, OFDM, COTS, Common Operational Picture, Common Tactical Picture, WLAN, Bridging, Tactical Internet, PRC-119, VHF, EPLRS, UHF			**15. NUMBER OF PAGES** 187
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN ANALYSIS OF IEEE 802.11B AND 802.16 TECHNOLOGIES AS PART OF THE TACTICAL INTERNET

Francisco A. Caceres
Captain, United States Marine Corps
B.A., University of Washington, 1999

Brad E. Swearingin
Captain, United States Marine Corps
B.S., Wright State University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2005**

Authors: Francisco A. Caceres

Brad E. Swearingin

Approved by: Rex Buddenberg
Thesis Advisor

Carl Oros
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research evaluates IEEE 802.11b and 802.16 technologies to determine how well they integrate into the tactical Internet. In order to establish a baseline, the current Marine Corps' systems architecture is analyzed with specific emphasis on mobile forces at the Regimental level and below. A side-by-side comparison of existing communication assets in the Marine Corps inventory, such as the Enhanced Position Location Reporting System (EPLRS) and Single Channel Ground and Airborne Radio System (SINCGARS), and available 802.11b/16 technologies can ascertain whether existing Command and Control requirements are met. Such a comparison can also determine the existence and extent of excess capacity and can identify potential adaptations required to implement commercial-off-the-shelf (COTS) technology into a military environment.

The method for side-by-side evaluation will incorporate both COTS products as well as Marine Corps tactical communication devices in laboratory as well as field experimentation. This research captures key performance metrics such as range, power consumption, security, and bandwidth but remains focused on the needs of the warfighter by evaluating the performance of the system in support of Command and Control Compact Edition (C2CE) and Command and Control Personal Computer (C2PC) applications.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- **A. BACKGROUND....1**
- **B. OBJECTIVES....7**
- **C. RESEARCH QUESTIONS....7**
- **D. SCOPE....8**
- **E. METHODOLOGY....8**
- **F. ORGANIZATION OF THESIS....9**

II. NETWORK CENTRIC WARFARE AND DISTRIBUTED OPERATIONS....11
- **A. NETWORK CENTRIC WARFARE....11**
- **B. DISTRIBUTED OPERATIONS....14**

III. OVERVIEW OF THE TACTICAL INTERNET....19
- **A. BACKGROUND....19**
  - **1. Radio Systems....19**
    - ***a. AN/MRC-142 Digital Wideband Transmission System (DWTS)....22***
    - ***b. AN/PSC-5 Satellite Radio....23***
    - ***c. Enhanced Position Location Reporting System (EPLRS)....25***
    - ***d. Single Channel Ground and Airborne Radio System (SINCGARS)....30***
    - ***e. AN/PRC-150 High Frequency Manpack Radio (HFMR)....35***
    - ***f. AN/PRC-113 Ultra High Frequency Radio....36***
    - ***g. AN/PRC-148 Tactical Handheld Radio - (THHR)....37***
    - ***h. Personal Role Radio....38***
    - ***i. Radio Systems Summary....39***
  - **2. Tactical Internet Nodes....39**
    - ***a. Dismounted Data Automated Communications Terminal (D-DACT)....41***
    - ***b. Mounted Data Automated Communications Terminal (M-DACT)....44***
    - ***c. Intelligence Operations Workstation (IOW)....47***
    - ***d. Intelligence Operations Server (IOS)....49***
    - ***e. Tactical Internet Node Summary....50***
  - **3. Tactical Internet Software Applications....50**
    - ***a. Command and Control Personal Computer (C2PC)....51***
    - ***b. Command and Control Compact Edition (C2CE....57***
    - ***c. Tactical Internet Software Applications Summary....61***
- **B. TACTICAL INTERNET SUMMARY....61**

IV. LEVERAGING IEEE 802.11B AND 802.16 WIRELESS TECHNOLOGIES....63
- **A. BACKGROUND....63**
- **B. HARRIS CORPORATION'S IEEE 802.11B BASED SECNET-11 PRODUCTS....65**

C. MOBILE AD-HOC NETWORKING (MANET) 75
1. Proactive MANET Protocols 75
2. Reactive MANET Protocols 75
3. Hybrid MANET Protocols 75
4. Optimized Link State Routing (OLSR) 76
D. CENGEN OLSR MODIFICATIONS 79
E. IEEE 802.16 PART 16: AIR INTERFACE FOR FIXED BROADBAND WIRELESS ACCESS SYSTEMS 82
F. REDLINE COMMUNICATIONS IEEE 802.16 BASED PRODUCTS 85
1. Setting Up and Configuring the AN-50e 86
2. Antenna Set-Up and Alignment for the AN-50e 91
3. AN-50e Field Terminal (FT) "Manpack" 92
4. Link Budget Calculation 95
5. Current Deployments of Redline Communications Equipment 96
G. TACTICAL ANTENNA MASTS 98
H. IXCHARIOT NETWORK ANALYSIS TOOL 99
I. MULTI-GENERATOR (MGEN) AND NETPROBE 101
J. SUMMARY 102

V. LABORATORY AND FIELD EXPERIMENTATION 103
A. COALITION OPERATING AREA SURVEILLANCE AND TARGETING SYSTEM (COASTS) EXPERIMENTS 103
1. Background 103
2. Network Architecture 104
3. Pre-Deployment Exercise (February 2005) 105
4. COASTS Deployment to Thailand (March 2005) 107
B. D-DACT TESTING AT CONSULTING AND ENGINEERING NEXT GENERATION NETWORKS (CENGEN) AND MARINE CORPS TACTICAL SYSTEMS SUPPORT ACTIVITY (MCTSSA) 109
1. Background 109
2. D-DACT Testing over Tactical Networks (November 2004) 110
3. D-DACT OLSR Demonstration (February 2005) 111
4. D-DACT OLSR Configuration and SecNet-11 COMSEC (April 2005) 115
C. SECNET-11 SWLAN AND REDLINE COMMUNICATIONS 802.16 POINT-TO-POINT LABORATORY TESTING WITH IXCHARIOT 116
1. Background 116
2. Network Architecture 116
3. Test Results 117
4. Summary 119
D. TACTICAL NETWORK TOPOLOGY FIELD EXPERIMENT (MAY 2005) 119
1. Background 119
2. Throughput as a Function of OLSR Hop Count 120
3. AN-50eFT Mobile Wireless Link 125
4. TNT Field Experiment 05-3 Summary 130

E. SECNET-11 SWLAN AND REDLINE COMMUNICATIONS 802.16 POINT-TO-MULTI-POINT LABORATORY TESTING WITH IXCHARIOT (SEPT 2005) 130
1. Background 130
2. Network Architecture 132
3. Test Results 134
a. Experiment #1 134
b. Experiment #2 135
4. Summary 137
F. SECNET-11 SWLAN AND REDLINE COMMUNICATIONS 802.16 POINT-TO-MULTI-POINT FIELD EXPERIMENT (SEPT 2005) 138
1. Background 138
2. Network Architecture 138
3. Test Results 139
4. C2PC Functionality 140
5. Summary 141

VI. ADAPT FROM COMMERCIAL-OFF-THE-SHELF (COTS) RECOMMENDATIONS 143
A. INTRODUCTION 143
B. ADAPT FROM COMMERCIAL-OFF-THE SHELF 143
1. Physical Layer 143
a. Frequency 143
b. Low Probability of Detection (LPD)/Low Probability of Interception 144
2. Form Factor 144
3. Antenna Deployment and Alignment 145
4. Automate the Promotion of a Subscriber Station 145
5. Information Assurance 146
C. SUMMARY 147

VII. CONCLUSION AND RECOMMENDATIONS 149
A. CONCLUSION 149
1. Problem Statement 149
2. Networking Requirements 150
3. Findings 150
B. FURTHER RESEARCH 150
1. Mobility 150
2. Layer 1 and 2 Security Solutions 151

LIST OF REFERENCES 153

BIBLIOGRAPHY 157

INITIAL DISTRIBUTION LIST 159

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Global Information Grid [2] 12
Figure 2. FORCEnet as the Enabler to NCW [6] 15
Figure 3. FORCEnet [7] 16
Figure 4. Voice and Data Distribution. Updated from: "Project Overview (April 2002)" by Major John Calvert EPLRS Project Officer Marine Corps Systems Command 21
Figure 5. MRC-142 Antenna in the Process of Being Deployed 22
Figure 6. AN/PSC-5 SATCOM Terminal with Collapsible High-Gain Antenna 23
Figure 7. AN/PSC-5 in Operation 24
Figure 8. EPLRS RT-1720C(C/G) 25
Figure 9. User's Readout (URO) 25
Figure 10. Sample EPLRS Network Diagram 27
Figure 11. Network Control Station (NCS) 29
Figure 12. ENM Version 10.X. 29
Figure 13. AN/PRC-119 Manpack Variant of the SINCGARS Family 30
Figure 14. Two Marines Deploy an OE-254 Antenna 34
Figure 15. AN/PRC-150 High Frequency Manpack Radio (HFMR) 35
Figure 16. AN/PRC-113 UHF Radio 36
Figure 17. AN/PRC-148 Tactical Handheld Radio (THHR) 37
Figure 18. Personal Role Radio (PRR) 38
Figure 19. Command and Control Personal Computer Node Connectivity 40
Figure 20. Dismounted Data Automated Communications Terminal (D-DACT) 41
Figure 21. Battery Adaptor 42
Figure 22. Memory Card 43
Figure 23. D-DACT Connected to Laptop via Serial Cable 43
Figure 24. D-DACT with External GPS Antenna 43
Figure 25. Mounted Data Automated Communications Terminal (M-DACT) 44
Figure 26. M-DACT Installed in a MRC-145 Vehicle 46
Figure 27. Intelligence Operations Workstation (IOW) 47
Figure 28. Toughbook CF-34 Damaged by 7.62mm Projectile in Iraq [16] 48
Figure 29. Combat Operations Center at Headquarters Battalion of 1st Marine Division. 49
Figure 30. Intelligence Operations Server (IOS) 49
Figure 31. Example Paper Map Board 52
Figure 32. 1:25,000 Scale CADRG Map 53
Figure 33. C2PC Overlay 54
Figure 34. Signal Composer Dialog Box 55
Figure 35. C2PC Sensor, Enemy and Friendly Tracks 56
Figure 36. Operation Areas Are Accessed from the Map Menu 58
Figure 37. C2CE Overlay 59
Figure 38. C2CE Preformatted Messages 59
Figure 39. C2CE File Receipt Alert 60

Figure 40. C2CE Friendly and Enemy Tracks 61
Figure 41. Tacticomp 64
Figure 42. Harris SecNet-11 PC Card 66
Figure 43. 802.11b Non-Overlapping Channel Allocation Adapted from Reference [22] 67
Figure 44. Distribution System with AP in Root Mode 68
Figure 45. Ad-Hoc Network 69
Figure 46. AN/CYZ-10 Data Transfer Device Connected to SecNet-11 PC Card 70
Figure 47. D-DACT with Protective Dome Removed and SecNet-11 Card Inserted 70
Figure 48. SecNet-11 PC Card with Two SMA Connectors 71
Figure 49. Packet Distribution During Flooding [24] 77
Figure 50. MPR Controlled Flooding [24] 78
Figure 51. Network Diagram for MANET Demonstration at CenGen 80
Figure 52. Starting CenGen's PocketPC OLSR Application 81
Figure 53. Launching CenGen's Windows 2000 and XP OLSR Application 82
Figure 54. OFDM Illustration [29] 84
Figure 55. Redline Communications' AN-50e 86
Figure 56. Laptop Connected to AN-50e at Ft. Ord 87
Figure 57. Default IP Address in Browser Address Bar 87
Figure 58. Username and Password Screen 88
Figure 59. AN-50e General Information Screen 88
Figure 60. System Configuration Screen 89
Figure 61. Max. Operational Power Per Channel (dBm) vs. Modulation [31] 90
Figure 62. North America: RF Channel Frequencies [31] 91
Figure 63. Two-Foot Flat Panel Antenna 91
Figure 64. One-Foot Flat Panel Antenna 91
Figure 65. AN-50eFT Manpack [32] 93
Figure 66. AN-50eFT Manpack Radio 93
Figure 67. GN-5 Portable, Mechanically-Cooled Germanium Gamma-Ray Spectrometer 94
Figure 68. Portable Fingerprint Solution 95
Figure 69. Redline Communications Deployed at Camp Fallujah, Iraq 97
Figure 70. Tactical Antenna Servicing the Redline Communications Base Station 99
Figure 71. IxChariot Console 100
Figure 72. COASTS Network Diagram 104
Figure 73. One-Foot Flat Panel Antenna at the Range Two Flight Line 108
Figure 74. D-DACT Network Evaluation 110
Figure 75. CenGen SecNet-11 SWLAN Network 112
Figure 76. CenGen OLSR MANET Functionality Demonstration 115
Figure 77. 802.11b/16 Lab Testing Experiment 116
Figure 78. D-DACT SWLAN Throughput Experiment 121
Figure 79. IXChariot Throughput Analysis as Hop Count Is Incremented 122
Figure 80. MGEN Packet Loss Analysis as Hop Count Is Incremented [31] 123
Figure 81. NetProbe Jitter Analysis as Hop Count Is Incremented [32] 124
Figure 82. SWLAN D-DACT Connectivity and IEEE 802.16 Wireless Backhaul 126

Figure 83. Light Reconnaissance Vehicle Redline 802.16 Suite 127
Figure 84. Light Reconnaissance Vehicle with Omni-Directional and Sector Antenna. 128
Figure 85. Common Operational Picture at the Company Gateway at 1634 24 May 2005..... 129
Figure 86. Proposed SWLAN with Redline AN-50e Point-to-Multi-Point Operation ... 131
Figure 87. IEEE 802.16 Composite Frame for TDD Systems Adapted from IEEE 802.16.3c-01/33r2 "OFDM Proposal for the IEEE 802.16a PHY Draft Standard" [33]..... 132
Figure 88. AN-50e Subscriber Stations and 40^{o} Sector Antenna in the Laboratory..... 133
Figure 89. AN-50e Base Station and Omni-Directional Antenna in the Laboratory..... 133
Figure 90. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Plot..... 134
Figure 91. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Plot (2^{nd} Run)..... 135
Figure 92. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Plot..... 136
Figure 93. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Plot (2^{nd} Run)..... 137
Figure 94. Fort Ord Point-to-Multi-Point Network Architecture..... 138
Figure 95. Fort Ord Point-to-Multi-Point IxChariot Throughput Plot..... 140
Figure 96. C2PC Screen Capture from A Co Gateway at 1630 2 Sept 2005..... 141

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. MAGTF Single Channel Radio Systems [9] 20
Table 2. EPLRS Network Hosts and Applications [12]....28
Table 3. SINCGARS Family of Tactical Radios Adapted from [10] 31
Table 4. Sample BN Radio Guard Chart....33
Table 5. SecNet-11 PCMCIA Power Output Measurements [23] 73
Table 6. 802.11b Range Example 74
Table 7. Antenna Specifications [30]....92
Table 8. Redline Communications Range Example 96
Table 9. Task and Measures of Effectiveness for COASTS Pre-Deployment Exercise....106
Table 10. CenGen D-DACT Evaluation Task List....113
Table 11. BN GW to Co GW (Wired Interface) Using 802.16 and Corresponding Plot....117
Table 12. Co GW to BN GW (Wired Interface) Using 802.16 and Corresponding Plot....118
Table 13. BN GW to Co GW (Wireless Interface) Using 802.16 and Corresponding Plot....118
Table 14. Co GW (Wireless Interface) to BN GW Using 802.16 and Corresponding Plot....118
Table 15. BN GW to D-DACT Using 802.16 and Corresponding Plot....119
Table 16. D-DACT to BN GW Using 802.16 and Corresponding Plot....119
Table 17. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Test....134
Table 18. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Test (2^{nd} Run)....135
Table 19. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Test....136
Table 20. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Test (2^{nd} Run)....136
Table 21. AN-50e Radio Deployment Characteristics....139
Table 22. Fort Ord Point-to-Multi-Point IxChariot Throughput Test Results....140

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AO	Area of Operations
AP	Access Point
ARQ	Automatic Repeat Request
BLOS	Beyond Line of Sight
C2CE	Command and Control Compact Edition
C2PC	Command and Control Personal Computer
C4	Command, Control, Communications and Computers
COASTS	Coalition Operating Area Surveillance and Targeting System
COP	Common Operational Picture
CONOPS	Concept of Operations
DAMA	Demand Assigned Multiple Access
DDACT	Dismounted Data Automated Communications Terminal
DO	Distributed Operations
DoD	Department of Defense
EPLRS	Enhanced Position Location Reporting System
FDD	Frequency Division Duplex
FRS	Family Radio Service
GIG	Global Information Grid
GIGA Lab	Global Information Grid Applications and Operations Code Laboratory
GPS	Global Positioning System
GWOT	Global War on Terrorism
HF	High Frequency
HIPERMAN	High Performance Radio Metropolitan Area Network
HMMWV	High Mobility Multipurpose Wheeled Vehicle
IEEE	Institute of Electrical and Electronics Engineers
IOS	Intelligence Operations Server

IOW	Intelligence Operations Workstation
IP	Internet Protocol
ISR	Intelligence, Surveillance, and Reconnaissance
JTRS	Joint Tactical Radio System
LAN	Local Area Network
LOE	Limited Objective Experiment
LOS	Line of Sight
LRV	Light Reconnaissance Vehicle
MAC	Medium Access Control
MAGTF	Marine Air-Ground Task Force
MANET	Mobile Ad-hoc Network
MCTSSA	Marine Corps Tactical Systems Support Activity
MDACT	Mounted Data Automated Communications Terminal
MSC	Major Subordinate Commands
NCW	Network Centric Warfare
NLOS	Non-Line of Sight
NOC	Network Operations Center
NPS	Naval Postgraduate School
OFDM	Orthogonal Frequency Division Multiplexing
OIF	Operation Iraqi Freedom
OLSR	Optimized Link State Routing
OTM	On-the-Move
PDA	Personal Data Assistant
PMP	Point-to-Multipoint
PRR	Personal Role Radio
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
R-PDA	Ruggedized Personal Data Assistant
SCR	Single-Channel Radio
SINCGARS	Single-Channel Ground and Airborne Radio System
SNMP	Simple Network Management Protocol

SOF	Special Operations Force(s)
SS	Subscriber Station
STAN	Surveillance, Targeting and Acquisition Network
TDD	Time Division Duplex
TDDS	Tactical Data Distribution System
THHR	Tactical Handheld Radio
TOC	Tactical Operations Center
TNT	Tactical Network Topology
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
USSOCOM	United States Special Operations Command
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WIBRO	Wireless Broadband
WIMAX	Worldwide Interoperability for Microwave Access

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Francisco Caceres – A sincere thank you for the continued love and support of my wife, Julie and our wonderful children who were extremely understanding of the time required to research and develop this thesis.

Brad Swearingin – I would like to thank my daughter Kathleen for her understanding of the last two years we have been apart. A special thanks to my parents who have always been there and supported me no matter what. And last, but not least, I would like to thank my loving wife, for her patience and support during this arduous process.

The authors would like to personally thank Rex Buddenberg and Carl Oros for their tremendous support and guidance throughout this process. We also extend our sincere thanks to Steven Durbano, Wayne Mandak, and John Jannucci from CenGen for sharing their time and expertise.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Over the course of the past decade the DoD has professed a strong correlation between net-centric warfare (NCW) and military success in publications such as Joint Vision 2020. Information superiority has even been debated as the latest Revolution in Military Affairs, and its application deemed a key component of the DoD's effort of transforming the force.

A Department of Defense Report to Congress dated 27 July 2001 concluded, "In the future, the network will be the single most important contributor to combat power," and that "NCW and Network Centric Operations should be the cornerstone of DoD's strategic plan for the transformation of the forces." [1]

A crucial element of a net-centric force is shared Situational Awareness (SA) and creation and maintenance of a Common Operational Picture (COP). Situational awareness is borne from communication systems that network sensors, small unit commanders, senior commanders in an Area of Responsibility (AOR), and offer oversight even to leaders in the Continental United States (CONUS). The decision-making and real-time collaboration among geographically dispersed commanders made possible through this seamless flow of information is the impetus behind investment in Command and Control Computers, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems.

Technological advances have allowed for computing devices to become feasible at even the lowest military echelons, and the proliferation of these new technologies has spawned the tactical Internet (TI). Since the mid-1990s, the United States Army and Marine Corps have developed both Single Channel Ground and Airborne Radio System (SINCGARS) and Enhanced Position Location Reporting System (EPLRS) radios in order to make the TI a reality on the modern battlefield. Operation Iraqi Freedom (OIF) has been the testing ground for these assets and initial reports are mixed. These latest digital Radio Frequency (RF) technologies present great promise and potential, but are routinely hampered by Line of Sight (LOS) limitations and bandwidth restrictions.

Because the most mobile users (Infantry Regiment and below) employ SINCGARS and EPLRS, these maneuver units routinely exceed LOS from adjacent, supporting, and higher commands. In addition to LOS limitations, maneuver forces employing SINCGARS and EPLRS are bandwidth constrained. Under the best conditions, an Ultra High Frequency (UHF) EPLRS radio is capable of 525 kbps and the Very High Frequency (VHF) SINCGARS is limited to 16 kbps.

A disparity of communications capability between major subordinate commands (MSCs) and tactical units (Regiment and below) has developed and is commonly referred to as the Digital Divide. This divide exists because MSC are equipped with communications assets with robust connections that deliver bandwidth in orders of magnitude greater than tactical units are able to receive with their data distribution via EPLRS and SINCGARS; therefore, information received at the MSC must be filtered if it is to be delivered to tactical units. Real-time video, video tele-conference (VTC), intelligence products, and even satellite communications are typically unavailable for mobile tactical units.

Due to the importance of providing SA and the COP to all echelons of command, new technologies must be analyzed and pursued in order to realize a true tactical Internet. Though the Joint Tactical Radio System (JTRS) is envisioned as the solution, existing data radio technologies should be leveraged today, as the fielding of JTRS is not expected prior to 2010.

This research evaluates Institute of Electrical and Electronics Engineers (IEEE) 802.11b and 802.16 technologies to determine how well these wireless technologies integrate into the tactical Internet. In order to establish a baseline, the current Marine Corps' systems architecture is analyzed with specific emphasis on mobile forces at the Regimental level and below. A side-by-side comparison between existing communication assets in the Marine Corps inventory, such as the Enhanced Position Location Reporting System (EPLRS) and Single Channel Ground and Airborne Radio System (SINCGARS), and available 802.11b/16 technologies will evaluate whether existing Command and Control requirements are met, will determine the existence and

extent of excess capacity, and will identify potential adaptations required to implement Commercial off-the-Shelf (COTS) technology into a military environment.

The method for side-by-side evaluation will incorporate both COTS products as well as Marine Corps tactical communication devices in the laboratory as well as field experimentation. This research captures key performance metrics such as range, power consumption, security, and bandwidth but remains focused on the needs of the warfighter by evaluating performance of the system in support of Command and Control Compact Edition (C2CE) and Command and Control Personal Computer (C2PC) applications.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

To a great extent the "transformation" occurring in the armed forces today is an effort to adopt new doctrine, techniques, tactics, and procedures that will allow our armed forces to capitalize on revolutionary changes in information systems of the past decade. Low-cost therefore plentiful, powerful, yet portable computational devices combined with significant increases in available bandwidth have provided the impetus for a force equipped with new computational devices networked with ever increasingly robust connections. What remains unaddressed is how to create a system that appropriately interconnects communications systems, computers, and most importantly the warfighter.

The future of this networked force has received a great deal of attention over the past decade through documents such as Joint Vision 2010 and more recently Joint Vision 2020 in which increased combat power is envisioned by capitalizing on information superiority. David S. Alberts, John J. Garstka, and Frederick P. Stein in their book, *Network Centric Warfare: Developing and Leveraging Information Superiority* define Network Centric Warfare (NCW) as "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization." [2]

The problem is that our current tactical communications have evolved to meet service specific and mission specific requirements. This artisan, pre-industrial specialization has created point-to-point systems that are highly inflexible and poorly support the interconnected environment required of today's distributed warfighters and decision makers, including coalition forces, allies and Non-Government Organizations (NGOs).

The origins of most of the tactical communication systems present on the battlefield today can be traced to Operations Desert Shield and Desert Storm, and in most

cases beyond that. These specialized systems are stressed beyond their limits to keep pace with a force that moves faster, strikes deeper, covers more expansive territory, and now produces and consumes more data.

Operation Iraqi Freedom (OIF) is the latest proving ground for our tactical communications assets and the results are mixed. Major Subordinate Commands (MSCs) have received unequaled bandwidth on the modern battlefield, by several estimates "42 times the bandwidth available to their counterparts in the first Gulf War." [3] This bandwidth has arrived in the form of real-time video from Unmanned Aerial Vehicles (UAVs), persistent and robust on the move communications with Iridium and International Maritime Satellite (INMARSAT) handsets, and access to the Global Information Grid (GIG) in the Continental United States (CONUS) via Standardized Tactical Entry Point (STEP) sites and Ground Mobile Forces (GMF) Super High Frequency (SHF) satellite systems.

The challenge remains in delivering high bandwidth, highly perishable information to disadvantaged users on the low bandwidth tactical Internet.

Several instances have been reported when time-critical information that could have substantially impacted blue and red force engagements or reduced blue-on-blue engagements were not delivered in a timely manner due to the digital divide, which is a disparity of communications capability among units on the battlefield. One example is the case of Lieutenant Colonel Ernest "Rock" Marone, the battalion commander with the 69th Armor of the Third Infantry Division. The incident, reported in *MIT Technology Review* in November 2004, focuses on a large-scale Iraqi counter attack along the Euphrates River bridge about 30 kilometers southwest of the City of Baghdad on the 2nd and 3rd of April 2003.

Lt Col Marone's force of 1,000 soldiers supported by 30 tanks and 14 Bradley fighting vehicles attacked across the bridge with virtually zero intelligence on the Iraqi defenders opposing them. The attack across the bridge was successful and the battalion assumed defensive positions to await reinforcements, yet the situation grew increasingly worse throughout the evening of the 2nd and the early hours of the 3rd. With little warning

from higher command, Lt Col Marone's unit was assaulted by three Iraqi Brigades of 5,000 to 10,000 soldiers supported by 25 to 30 tanks and 70 to 80 armored personnel carriers.

For all the technological advances and robust networks employed by higher echelons of command, Lt Col Marone and his men received insufficient warning of the impending attack and discovered the size and disposition of the enemy upon contact. An assessment on operations during OIF I by senior researchers at Rand was that "at the division level or above, the view of the battle space was adequate to their needs. They were getting good feeds from their sensors, but amongst front line army commanders like Marone-as well as his counterparts in the U.S. Marines-everybody said the same thing. It was a universal comment: 'We had terrible situational awareness.'" [3] This lack of situational awareness can be attributed to two factors. One is that higher headquarters had the information, but did not pass it down through the appropriate channels in a timely manner. Factor two can be attributed to lack of sensors and robust on-the-move communications. This thesis proposes that a major contributing factor to this poor situational awareness is the lack of a reliable wideband communication system.

Although static or fixed communications assets have greatly enhanced the connectivity of major subordinate commands through the infusion of Global Broadcast Systems (GBS), Deployable KU Earth Terminals, Ground Mobile Forces assets such as AN/TSC-93, optical fiber and wireless Data Distribution Systems (DDS), and a hosts of sensors, these robust connections and systems have generally been beyond the reach of small unit commands (regiment and below). The tactical Internet has been developed to provide data distribution to the "last tactical mile" to small unit forces, but due to their small footprint and high degree of mobility, meeting these communications needs have challenged the services.

Small units accomplish all their voice and data connectivity with small, lightweight communication assets that are either manpackable or vehicle mounted; however, these portable devices lack the power required or the ability to deploy high-gain antennas to support higher bandwidths. Additionally, these systems are Line of Sight (LOS) dependant; therefore, service is routinely interrupted because of terrain or because

the units are physically separated by distance. Previous generations of lightweight communications have not been routable, providing no multi-cast and limited inter-networking capability.

Two primary assets form the backbone of the tactical Internet for the Infantry Regiment and below, the Single Channel Ground and Airborne Radio System (SINCGARS), and the Enhanced Position Location Reporting System (EPLRS). When released to the fleet in the early 1990s, SINCGARS was a substantial enhancement over the AN/PRC-77, which was the workhorse of the Vietnam Conflict; however, SINCGARS is scheduled for replacement by the Joint Tactical Radio System in order to support operators who need to exchange time-sensitive information in addition to voice traffic. EPLRS represents a system upgrade to the original PLRS project, which was designed to provide Position Location Information (PLI) now delivered by Global Position Satellite (GPS) receivers. Today EPLRS is the primary tactical data network for the Infantry Regiment and below. These systems, which in effect are proprietary point-to-point, fail to deliver the flexibility, adaptability, scalability, and bandwidth required of the Network Centric Force.

Future warfighting concepts such as Distributed Operations (DO), which seek to "realize the full potential of the small unit leader," overtax the capabilities of current communications assets. Empowered with precise intelligence, greater situational awareness via a common operational picture (COP), and a well defined commander's intent, these distributed units are capable of independent action. The Joint Tactical Radio System (JTRS), a software defined radio, is purported as the future of tactical communications; however, the system is not envisioned for fielding to the operating forces until fiscal year 2010 at the earliest.

The desire to leverage technology capable of supporting this vision requires rigorous experimentation of a wide array of communications systems to find those that will best arm tomorrow's warfighter for success in the "internetworked" battlefield. This research is an attempt to apply field experimentation and to integrate USMC communications systems employed in the fleet today, such as the Dismounted Data

Automated Communications Terminal (D-DACT), to wireless technologies previously analyzed by Naval Postgraduate School students.

This research focuses on a small but very important portion of the overall Global Information Grid (GIG), namely the communication links to small units in the DO environment. Units employing distributed operations will require capabilities that extend across the six warfighting functions:

1. *Maneuver*: Distributed operations will require both air mobility and organic vehicles for ground mobility. In order to exploit intelligence, individual units must move rapidly to maintain positional advantage relative to the enemy or to enhance force protection measures. [4]

2. *Fires*: Distributed operations by networked forces will potentially generate significant amounts of actionable intelligence. Small units will exploit this intelligence by using both enhanced direct fire capabilities and supporting arms to neutralize or destroy much larger forces. [4]

3. *Intelligence*: Although the distributed operations concept does not focus on reconnaissance, it nonetheless underscores the importance of individual Marines and small units in generating intelligence for their own use, as well as for higher headquarters. It is important to realize that the human dimension manifested in small units may be the only means to identify our adversaries positively and to gain an insight into their likely intent. [4]

4. *Command and Control*: A robust and resilient network will enable this operating approach. This network will include over-the-horizon, on-the-move, and beyond-line-of sight communications assets that connect commanders to distributed units and provide connectivity throughout the force, to include, where applicable, the sea-based elements of that force. [4]

5. *Logistics*: Units operating in widely dispersed manner will require unique combat logistics support, especially in supply, maintenance, and health services. The supply chain must be highly adaptive and flexible. [4]

6. *Force Protection*: In the case of protection against enemy action, an increased degree of force protection is inherent in distributed operations, because dispersion itself is a protective measure. However, dispersion beyond the range of mutual support with direct-fire weapons could potentially increase vulnerability. [4]

This research evaluates Institute of Electrical and Electronics Engineers (IEEE) 802.11b and 802.16 technologies to determine whether these wireless technologies can integrate into the tactical Internet. Harris SecNet-11 Personal Computer Memory Card International Association (PCMCIA) cards were used to provide a Secure Wireless Local Area Network (SWLAN) to simulate the deployment of a Marine Rifle Company's D-DACTs. During experimentation the SWLAN varied in size from two to eight D-DACTs. Redline Communications pre-802.16 equipment was used to backhaul SWLAN traffic to a mobile command and control vehicle simulating current communications techniques, such as AN/MRC-142 vehicular retransmission teams. Lastly, 802.16 links were employed to backhaul the SWLAN traffic to a simulated Combat Operations Center (COC).

A critical element of this study was a partnership with Steven Durbano, Jon Jannucci, and Wayne Mandak from Consulting and Engineering Next Generation Networks (CenGen). This research firm, based in Columbia MD, mans a small office in Carlsbad, CA, and is involved in a project sponsored by the Office of Naval Research to address secure wireless connectivity for the Navy and Marine Corps. They have developed Mobile Ad-hoc Network (MANET) functionality for the Harris SecNet-11 card using the Optimized Link State Routing (OLSR) protocol. This MANET functionality augments 802.11b networks by providing a redundant, self-forming, self-healing network to deliver robust and reliable communications paths. Their work to date provides MANET functionality to IOWs running Windows 2000, and Windows XP, as well for the M-DACT and D-DACT running Windows NT and WinCE 2003 operating systems.

In order to establish a baseline for the performance of these wireless technologies, we analyzed current Marine Corps' systems architecture with specific emphasis on mobile forces at the Regimental level and below. A side-by-side comparison between SINCGARS, and EPLRS radios was conducted, and the wireless technologies were integrated into SINCGARS and EPLRS networks to demonstrate that they could operate as part of the tactical Internet. The intent of this research was to evaluate whether existing Command and Control requirements were met, determine the existence and extent of excess capacity, and identify potential adaptations required to implement Commercial-off-the Shelf (COTS) technology into a military environment.

This research required both laboratory and field experimentation in order to capture key performance metrics such as bandwidth as a function of range, bandwidth as a function of hop count, power consumption, and security requirements, but remained focused on the needs of the warfighter by evaluating performance of the system in support of Command and Control Compact Edition (C2CE) and Command and Control Personal Computer (C2PC) applications.

B. OBJECTIVES

This research evaluates COTS IEEE 802.11b and 802.16 wireless technologies to determine whether a SecNet-11 SWLAN with embedded MANET functionality could integrate into the tactical Internet, support the current communications architecture, and provide a robust, reliable communications path for the Dismounted Digital Automated Communications Terminal.

C. RESEARCH QUESTIONS

1. Can IEEE 802.11b and IEEE 802.16 wireless technologies be leveraged in order to support and to augment command and control requirements currently delivered by those devices that comprise the tactical Internet?

2. What advantages and disadvantages do IEEE 802.11b and IEEE 802.16 technologies present when compared to current communication assets? Variables of particular interests are range, power consumption, security, bandwidth, and channel interference.

3. Given the results of the last question, what specific adaptations will be required for COTS IEEE 802.11b and IEEE 802.16 technologies to meet military specifications?

D. SCOPE

The scope of this thesis will include:

1. A review of the United States Marine Corps' current systems architecture for those assets that comprise the tactical Internet. This review, in addition to an analysis of the current operational architecture, will help determine the typical traffic profile of these links.

2. An analysis of commercially available IEEE 802.11b and IEEE 802.16 wireless technologies to present solutions that can be leveraged to provide additional data connectivity to the warfighter.

3. Laboratory and field experimentation to test current USMC communications assets side-by-side with IEEE 802.11b and IEEE 802.16 equipment to measure performance relative to variables of interest (i.e. range, power consumption, security, bandwidth, and channel interference).

4. An analysis of adaptations to commercial IEEE 802.11b and IEEE 802.16 technologies required prior to implementation in a tactical military environment.

E. METHODOLOGY

1. Research DoD and USMC publications, orders, Training Manuals for USMC communications assets, and the Marine Corps Architecture Support Environment for architecture data in order to collect the information required to present the existing USMC operational and systems architecture.

2. Research documentation from the IEEE and industry sources on 802.11b and 802.16 technologies in order to collect the information required to procure, install, operate, and maintain a wireless network to evaluate and compare with existing USMC communications assets.

3. Perform controlled tests to gain familiarity with both USMC communications assets and IEEE 802.11b and IEEE 802.16 technologies.

4. Perform controlled tests to collect key metrics for comparisons between existing tactical Internet communications assets and IEEE 802.11b and IEEE 802.16 technologies.

5. Provide relevant analysis and comparison between observed results of side-by-side testing of USMC communications assets and IEEE 802.11b and IEEE 802.16 technologies.

F. ORGANIZATION OF THESIS

CHAPTER I. Introduction: This chapter discusses the problem and provides background information on the tactical Internet. The problem addresses the fundamental reason for conducting this research, and provides a basic introduction to different systems that are to be studied.

CHAPTER II. Network Centric Warfare and Distributed Operations: This chapter highlights a new concept of operation under analysis by the Marine Corps Warfighting Laboratory, which focuses on the communications requirements of small, highly agile units capable of independent action through improved command and control (C2) processes. This vision of future forces is consistent with the concept of Network Centric Warfare and focuses on the requirements of those units discussed in this research. Those forces that today use the tactical Internet.

CHAPTER III. Overview of the tactical Internet**:** This chapter provides an overview of the communication systems, computer nodes, and software applications used by the Marine Air Ground Task Force (MAGTF) in the execution of assigned tasks. This chapter builds an understanding of the tactical Internet in its current implementation, and provides an operating environment for comparison against IEEE 802.11b and 802.16 wireless technologies.

CHAPTER IV. Leveraging IEEE 802.11b and 802.16 Wireless Technologies: This chapter provides an overview of the IEEE 802.11b and 802.16

technologies used during this thesis research. This chapter presents the technologies that are further reported in Chapter V during the experimentation phase.

CHAPTER V. Laboratory Field Experimentation: This chapter discusses what laboratory and field experiments where conducted as well as the results obtained.

CHAPTER VI. Adapt from COTS Recommendations: This chapter recommends modifications to COTS IEEE 802.11b and 802.16 products. These recommendations are generated from the experience gained during this thesis research and operational experience of the authors.

CHAPTER VII. Conclusion and Recommendations: This chapter provides a conclusion for the research study as well as articulates areas that warrant further analysis through future research.

II. NETWORK CENTRIC WARFARE AND DISTRIBUTED OPERATIONS

A. NETWORK CENTRIC WARFARE

The concept of Network Centric Warfare (NCW) has existed for several years. The term was first introduced in 1998 in the article "Network Centric Warfare: Its Origins and Future" and later gained momentum in 1999 with the book that was mentioned earlier: Network Centric Warfare: Developing and Leveraging Information Superiority. Since then, DoD has adopted it as the warfighting concept that will achieve Joint Vision 2020 operational capabilities.

NCW is about human and organizational behavior and is based on novel concepts that increase the efficiencies of military operations. NCW is a concept that intends to capitalize on of the Information Age[1] and transform the Department of Defense (DoD) through the networking of spatially separate entities by using the Global Information Grid (GIG)[2], shown in Figure 1. [2] The GIG will increase situational awareness, provide more timely and accurate intelligence, and increase the tempo of operations.

---

[1] The Information Age is a term applied to the period when movement of information became faster than physical movement, more narrowly applied to the late 20th century (post 1970) and early 21st century. It is often used in conjunction with the term post-industrial society.

[2] The Global Information Grid (GIG) is a grid computing network for the United States military. It is the physical manifestation of the network-centric warfare doctrine. The GIG was envisioned by the Department of Defense Chief Information Officer on September 22, 1999 and was officially mandated by an overarching directive from the Deputy Secretary of Defense on September 19, 2002.

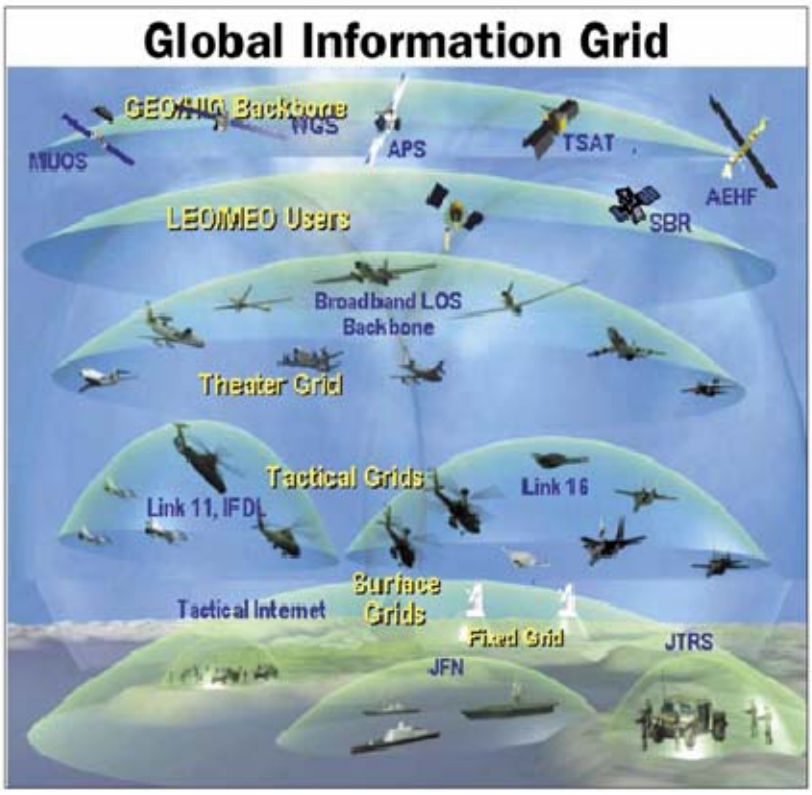

Figure 1. Global Information Grid [2]

Several key concepts define NCW. One concept is that entities in the battlespace are effectively linked. This linking requires a robust, high-performance information infrastructure that provides all elements of the warfighting enterprise with access to high-quality information services. Another key concept is that our force is knowledgeable. Empowered by knowledge, derived from a shared awareness of the battlespace and a shared understanding of the commanders' intent, our forces will be able to self-synchronize, and be more effective when operating autonomously. The last major concept in defining NCW is the use of a geographically dispersed force. The Information Age has made it possible to free the source of combat power from the physical location of battlespace assets and will allow forces to be more effective while on the move. These following basic concepts comprise the tenets of NCW:

1. A robustly networked force improves information sharing
2. Information sharing and collaboration enhance the quality of information and shared situational awareness
3. Shared situational awareness enables self-synchronization
4. These, in turn, dramatically increase mission effectiveness.

In the book Network Centric Warfare: Developing and Leveraging Information Superiority, the authors attempt to dispel a few myths surrounding NCW. Understanding some of these myths and realizing some of the hurdles is important. The following are a few myths taken from the book:

1. Myth: "NCW predominantly concerns the network." Obviously a network does need to exist for NCW to thrive, but it is more about networking than networks. It pertains to the increased combat power that can be generated by a network-centric force. NCW is derived from effective linking of knowledgeable entities that are geographically dispersed. The networking of knowledgeable entities enables them to share information and to collaborate to develop shared awareness and also to collaborate with one another to achieve a degree of self-synchronization. [2] For example, the combination of digitization and networking can be employed to develop a common operational picture that reduces the ambiguity and confusion of combat by identifying the positions of friendly forces and the known positions of the enemy clearly. [5]
2. Myth: "NCW is an attempt to automate war that can only fail." NCW is not about turning the battle over to "the network" or even about relying more on automated tools and decision aids. It really involves exploiting information to maximize combat power by effectively and efficiently employing one's available information and warfighting assets. [2]
3. Myth: "NCW will result in our chasing our tails rather than responding to battlespace events." The concern is that we will develop such a rapid pace

that we will get ahead of ourselves on the battlefield, responding to ourselves instead of an adversary's actions. But in many circumstances and missions with all factors being equal speed of command will be decisive. NCW gives us the opportunity to increase speed of command when it is appropriate, and it does not force us to do so when it is not. [2]

4. Myth: "NCW will not survive first contact with the real fog, friction, and complexity of war." The fact that warfare will always be characterized by fog, friction, complexity, and irrationality circumscribes but does not negate the benefits that network-centric operations can provide to the forces in terms of improved battlespace awareness and access to distributed assets. Although predicting human and organizational behavior will remain well beyond one's capabilities, having a better near real-time picture of what is happening certainly reduces a lot of uncertainty. [2]

NCW is not really new. It is just becoming more of a reality as technology improves and advances. NCW is about capitalizing on the potential being offered by this rapid advancement in information technology. In order for this to happen, the parts that make up this GIG need to be integrated and interoperable amongst one another. As DoD moves forward, the appropriate doctrine must be in place to take advantage of these advancements.

B. DISTRIBUTED OPERATIONS

Distributed Operations (DO) is the next logical step for the Marine Corps in taking full advantage of a networked battlespace. General Hagee, the 33rd Commandant of the Marine Corps, recently approved the concept of DO and wrote "Distributed Operations describes an operating approach that requires new ways to educate and train our Marines and that guides us in the use of emerging technologies." [4] DO also describes an operating approach that will create an advantage over an adversary through the deliberate use of physically being separated and the coordinated, interdependent, tactical actions enabled by increased access to functional support, as well as by enhanced combat capabilities at the small unit level.

DO constitutes a form of maneuver warfare. Small, highly capable units spread across a large area of operations will provide the spatial advantage desired in maneuver warfare, in that they will be able to sense an expanded battlespace and can use close combat or supporting arms, including joint fires, to disrupt the enemy's access to key terrain and avenues of approach. [4] In the tactical application of the distributed operations concept, it is envisioned that maneuver units will operate in disaggregated ways, with companies, platoons, and even squads dispersed beyond the normal range of mutually supporting organic direct fires, but linked through a command and control network. The ability to reaggregate will be enabled by focused and energetic cross training of small units, the creation and use of a more robust communications capability for small units, and an increase in the number of tactical mobility assets available for small units. [4]

DO capabilities will be complementary. Units employing these techniques will deploy and fight in coordination with other units using conventional tactics. One example would be sea-based forces projecting power using ship-to-objective maneuver (STOM), with units operating in an aggregated manner being augmented by other units using distributed operations procedures. [4] DO will fit under the umbrella of FORCEnet, which is the enabler that makes NCW possible for the Navy and Marine Corps, as shown in Figure 2. [6]

Figure 2. FORCEnet as the Enabler to NCW [6]

Under the FORCEnet umbrella, Expeditionary Maneuver Warfare (EMW), the Marine Corps' capstone concept is accomplished by employing the operational concepts of Operational Maneuver from the Sea (OMFTS), STOM, and Sustained Operations Ashore (SOA) in conjunction with the three pillars of Sea Power 21. DO is a concept that will align with STOM and give the regional combatant commander (RCC) more options in the battlespace. FORCEnet ensued from the Navy's Sea Power-21. Sea Power-21 is the Navy's vision to align, organize, integrate, and transform the Navy to meet the challenges that lie ahead. Sea Power-21 is based on three pillars: Sea Strike, Sea Shield, and Sea Basing, which will employ current capabilities in new ways, introduce innovative capabilities as quickly as possible, and achieve unprecedented maritime power. [7]

Below is an excerpt taken from U.S. Navy Proceedings by Admiral Vern Clark about these three pillars and the vision of Sea Power-21

> Sea Strike, Sea Shield, and Sea Basing will be enabled by FORCEnet, an overarching effort to integrate warriors, sensors, networks, command and control, platforms, and weapons into a fully netted, combat force. FORCEnet is like the glue that unites them. Network-centric warfare has been studied for a decade, and FORCEnet will be the Navy's plan to make it an operational reality. FORCEnet, Sea Strike, Sea Shield, and Sea Basing capabilities will be deployed by way of a Global Concept of Operations that widely distributes the firepower of the fleet, strengthens deterrence, improves crisis response, and positions us to win wars decisively. [7]

Figure 3 below, illustrates the three pillars tied together by FORCEnet:

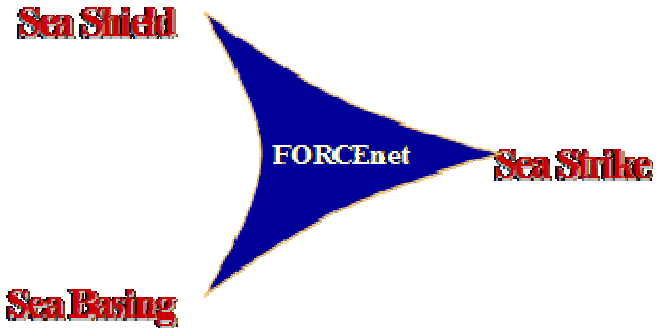

Figure 3. FORCEnet [7]

As mentioned earlier, this thesis focuses on a small aspect of an expansive picture, namely the communication links to the small units in the DO. Recently, in a report released by the Marine Corps Warfighting Laboratory, which assessed this new concept of distributed operations, a few concerns needed to be addressed. One, which is a recurring theme in many areas, is the need for more bandwidth. The wargame participants noted that the communications suite planned for this exercise lacked sufficient bandwidth to exchange imagery. [8] Another significant conclusion derived from the wargame participants was that a broad implementation of a DO capability is highly dependent on the availability of satellite-based communications systems. Currently the right equipment and architecture is not available in the Marine Corps to handle the needs of the tactical user in distributed operations. DoD is on the right track in developing the communications equipment and the architecture to accommodate it, but it will take several years before it becomes reality. In this thesis, alternative solutions are proposed for several technologies available today for securing the bandwidth needed for the tactical user in distributed operations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. OVERVIEW OF THE TACTICAL INTERNET

A. BACKGROUND

This chapter will cover the communication assets, computer terminals, and software applications used by elements of the Marine Air Ground Task Force (MAGTF) to conduct operations in a tactical environment. The intent is to provide a high-level overview of these systems, not a detailed technical analysis; an in-depth review of these systems is beyond the scope of this thesis. This overview is provided in order to establish the equipment available to maneuver forces for the purposes of command and control, as well as to present the type of information typically delivered over these systems. This is relevant to understand the environment of future wireless technologies. This overview begins with the following discussion of eight radio systems, followed by information on computing assets, and finishes with information on key software applications.

1. Radio Systems

At the regiment level and below, distribution of voice and digital information is primarily accomplished through Single Channel Radio (SCR). SCR systems operate in the High Frequency (HF), Very High Frequency (VHF), and Ultra High Frequency (UHF) bands of the electromagnetic spectrum. (Table 1) The communication systems employed at this echelon of command vary drastically from those employed at higher headquarters. Large commands, Marine Expeditionary Force (MEF) or Division move less frequently than units at the regiment or below; therefore, the systems they operate exploit the benefits of fixed positions.

Frequency Band	MAGTF SCR Equipment Used	Operating Frequency Range	Typical Application
HF	AN/PRC-150 AN/GRC-193 AN/MRC-138	2-29.999 MHz	Radio line of sight and beyond/long range
VHF	AN/PRC-150	2-60 MHz	Radio line of sight
	SINCGARS Family	30-88 MHz	Radio line of sight and relay/retansmission
	THHR	30-512 MHz	Radio line of sight
	AN/PRC-113 AN/VRC-83	116-150 MHz	Critical line of sight (ground to air)
UHF	THHR	30-512 MHz	Radio line of sight
	AN/PRC-113 AN/VRC-83 AN/GRC-171	225-400 MHz	Critical line of sight (ground to air)
	AN/PSC-5		SATCOM footprint
	EPLRS	20-450 MHz	Line of sight
	AN/MRC-142	1350-1850 MHz	Terrestrial line of sight multi-channel radio
	PRR	2.4 GHz	Intra Team communication

Table 1. MAGTF Single Channel Radio Systems [9]

Deploying communication systems at static positions allows for the use of better sources of power, either alternating current (AC) from physical structures or direct current (DC) from generators, as well as the deployment of physically larger antennas that deliver greater antenna gain. Less frequent displacements allow time for complex radio systems to be installed and operated whereas highly mobile units would receive no benefit from setting up these complex systems only to dismantle them.

This model is applicable further down the chain of command as well. Infantry battalions exhibit greater mobility than regiments, companies are more mobile than battalions, and so on. SCR systems were designed to support the requirements of highly mobile forces vice units that can operate from fixed positions. The SCR assets employed at the regiment level and below use smaller collapsible omni-directional antennas, and 12-volt Lithium batteries for on-the-move communications and require a smaller footprint in terms of physical space, personnel, and logistical support. The direct impact of the compromises made to support mobile users is that their systems become less capable in terms of available bandwidth.

This model of greater mobility but decreasing capability will become evident as radio assets are discussed in the subsequent section; therefore, this short overview of radio systems will trace the organizational structure from Regiment to Battalion, Company, Platoon, and Squad. This overview entails the aspects presented in Figure 4 below, which shows the communications architecture for Marine units and is referenced throughout this section to illustrate the systems.

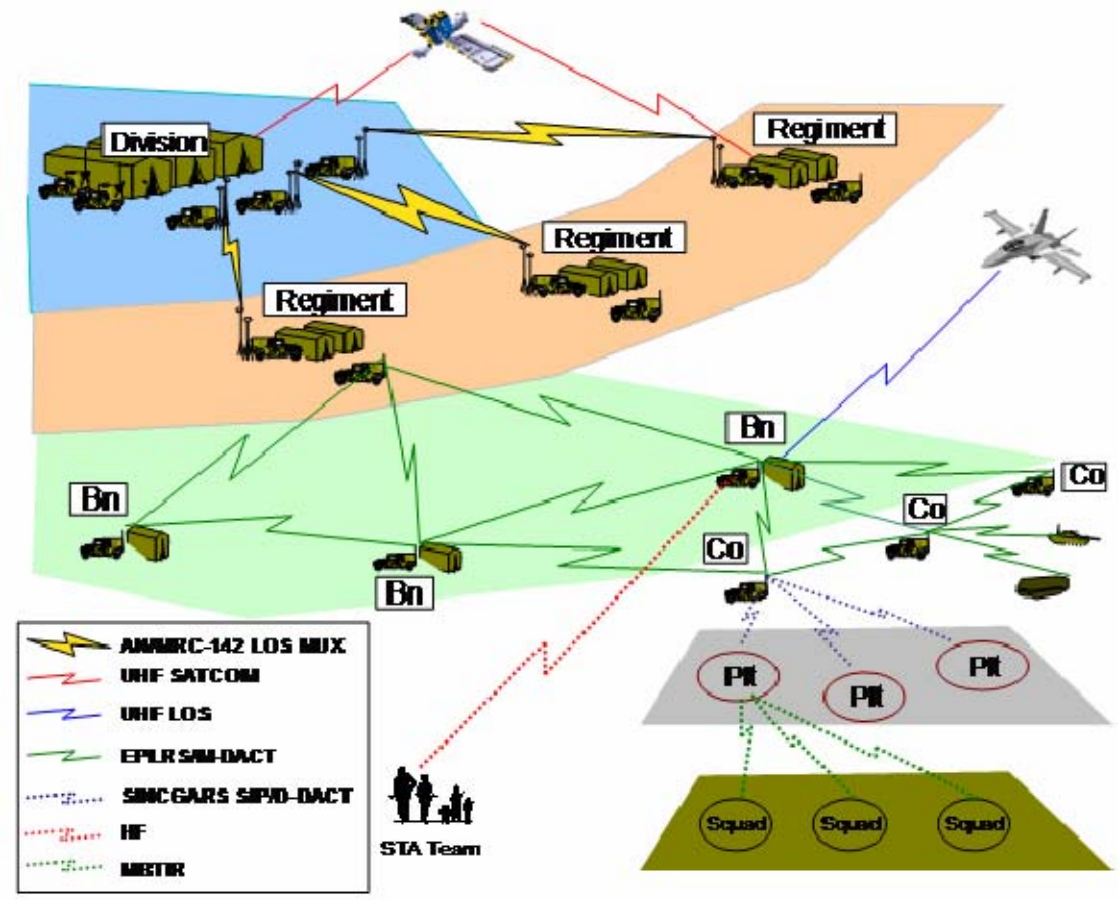

Figure 4. Voice and Data Distribution. Updated from: "Project Overview (April 2002)" by Major John Calvert EPLRS Project Officer Marine Corps Systems Command

a. AN/MRC-142 Digital Wideband Transmission System (DWTS)

Initially fielded in 1993, the AN/MRC-142 is a UHF terrestrial line-of-sight multi-channel radio system operating in the 1350 to 1850 MHz range. The system is integrated into a High Mobility Multipurpose Wheeled Vehicle (HMMWV). The MRC-142 provides a two-way secure digital wideband transmission with a range up to 35 miles consisting of eight channels with selectable rates of either 16 or 32 kbps, for a maximum data rate of 576 kbps using an FCC-100 multiplexer. The Marine Corps has procured around 400 MRC-142s, which are fielded to the Regiment level or above. [10]

Multi-channel radios are complex systems that require additional expertise to operate than Single Channel Radios. As such the MRC-142 requires a team of three to four operators and approximately 30 minutes of set-up time to prepare for operations. The system does not support on-the-move communications. High-gain parabolic grid antennas mounted on 50' masts, pictured in Figure 5 below, are deployed and aimed at a second MRC-142 system. Therefore line-of-sight is a critical requirement for this UHF radio system.

Figure 5. MRC-142 Antenna in the Process of Being Deployed

The concept of operation for these systems calls for each Major Subordinate Command within the Division (Ground, Air, and Combat Service Support) to deliver one end of the link (one MRC-142 system with appropriate personnel). The

Division provides the second MRC-142 system located at Division headquarters. This point-to-point link is demonstrated in Figure 4 with the Division delivering one MRC-142 link to each of its three Regiments. This multiplexed link can deliver secure tactical telephone, multiple data networking services, (e.g. SIPRNET, NIPRNET, CWAN, etc), and special circuits and services (VTC, JWICS, etc).

b. AN/PSC-5 Satellite Radio

Figure 6. AN/PSC-5 SATCOM Terminal with Collapsible High-Gain Antenna

Initially fielded in 1997, the PSC-5 terminal, pictured in Figure 6 above, is a UHF/VHF Manpack Line-of-Sight and SATCOM/DAMA (Demand Assigned Multiple Access) Terminal that can operate in the following bands:

LOS 30.000 to 399.975 MHZ

SATCOM 225.000 to 399.995 MHZ

DAMA 225.000 to 399.995 MHZ

This manpack terminal employs both narrowband (5 KHz) and wideband (25 KHz) channels capable of supporting data rates of 2.4 and 16 Kbps respectively. The PSC-5 serves as the primary Tactical Satellite command and control Single Channel Radio for the MAGTF and is used to extend lines of communications for critical voice communications nets. The PSC-5 is illustrated in operation in Figure 7 below.

Figure 7. AN/PSC-5 in Operation

The Marine Corps procured 589 PSC-5 terminals and fielded the systems to the regiment level and above. The most common method of employment is Demand Assigned Multiple Access, one of several multiple access schemes employed to share limited satellite access more efficiently. With demand assignment, the user makes a channel request, and after a brief time lag, a channel is allocated. [10]

Due to the limited available bandwidth of tactical satellite resources, these systems are employed to support critical long-range communications requirements. Typical deployments support deep reconnaissance teams or critical communication links between higher headquarters and subordinate commands. Figure 4 demonstrates a SATCOM link between division and regiment and might support Division Tactical Net #1 commonly annotated as "Div Tac1."

Despite the PSC-5's ability to deliver data traffic, it is generally operated as a voice circuit. This system is operated by a single user and requires additional training than that required of other Single Channel systems. As is evident in Figure 7, the PSC-5 antenna does not support on-the-move communications. The high-gain collapsible antenna must be erected and aimed at the appropriate azimuth and elevation in order to establish connection with supporting satellites overhead.

c. Enhanced Position Location Reporting System (EPLRS)

Figure 8. EPLRS RT-1720C(C/G)

EPLRS is an Ultra-High Frequency (UHF) system that operates at 20 to 450 MHz. EPLRS is a line-of-sight terminal capable of providing links of six miles in ground-to-ground or 62 miles in ground-to-air deployments. EPLRS is a Tactical Data Radio that provides secure, jam-resistant radio frequency connectivity using a Time Division Multiple Access (TDMA) scheme. The EPLRS radio supports four types of interfaces, the Army Data Distribution System Interface (ADDSI), Military Standard-1553B (MIL-STD-1553B), Point-to-Point (PPP), and Ethernet. [11]

The main components of the Radio Set are a receiver-transmitter (RT) (RT-1720C(C)/G) (See Figure 8 above), an Enhanced Dual Power Adapter (EDPA), and a User's Readout (URO) device for entering and receiving messages. (See Figure 9)

Figure 9. User's Readout (URO)

EPLRS is the main source of tactical data connectivity between the Regiment and its Battalions. Two primary Combat Radio Nets are employed to meet

operational requirements. The first is a Command and Control (C2) net to deliver the Common Tactical Picture (CTP) to Command and Control Personal Computer (C2PC) client machines typically referred to as Regt CTP. (The C2PC application is discussed in further detail in a subsequent section). The second is the Fire Support Coordination (FSC) net, which allows for Advanced Field Artillery Tactical Data Systems (AFATDS) connectivity between the Regt Fire Support Coordination Center and Fire Direction Center terminals. This net is typically referred to as Regt Fires.

Regiment and Battalion EPLRS radios are configured for a Carrier Sense Multiple Access (CSMA) scheme where Regt CTP and Regt Fires nets receive 7.2 kbps and 14.4 kbps segments of the available 56 kbps bandwidth respectively. The most recent system upgrade delivers 525 kbps providing greater bandwidth to these two critical networks.

During Regimental exercises in which Capt Caceres participated as the Communications Officer for the 2nd Battalion, 3rd Marines, the Regt CTP net supported eight to ten EPLRS radios on a CSMA architecture. At the battalion level the EPLRS radios were used at the battalion main combat operations center, in the Battalion Commander's, Operations Officer's (S-3), and Executive Officer's AN/MRC-145 vehicles. An EPLRS network diagram for the Regimental exercise Hawaiian Combined Arms Exercise (HCAX) is provided in Figure 10.

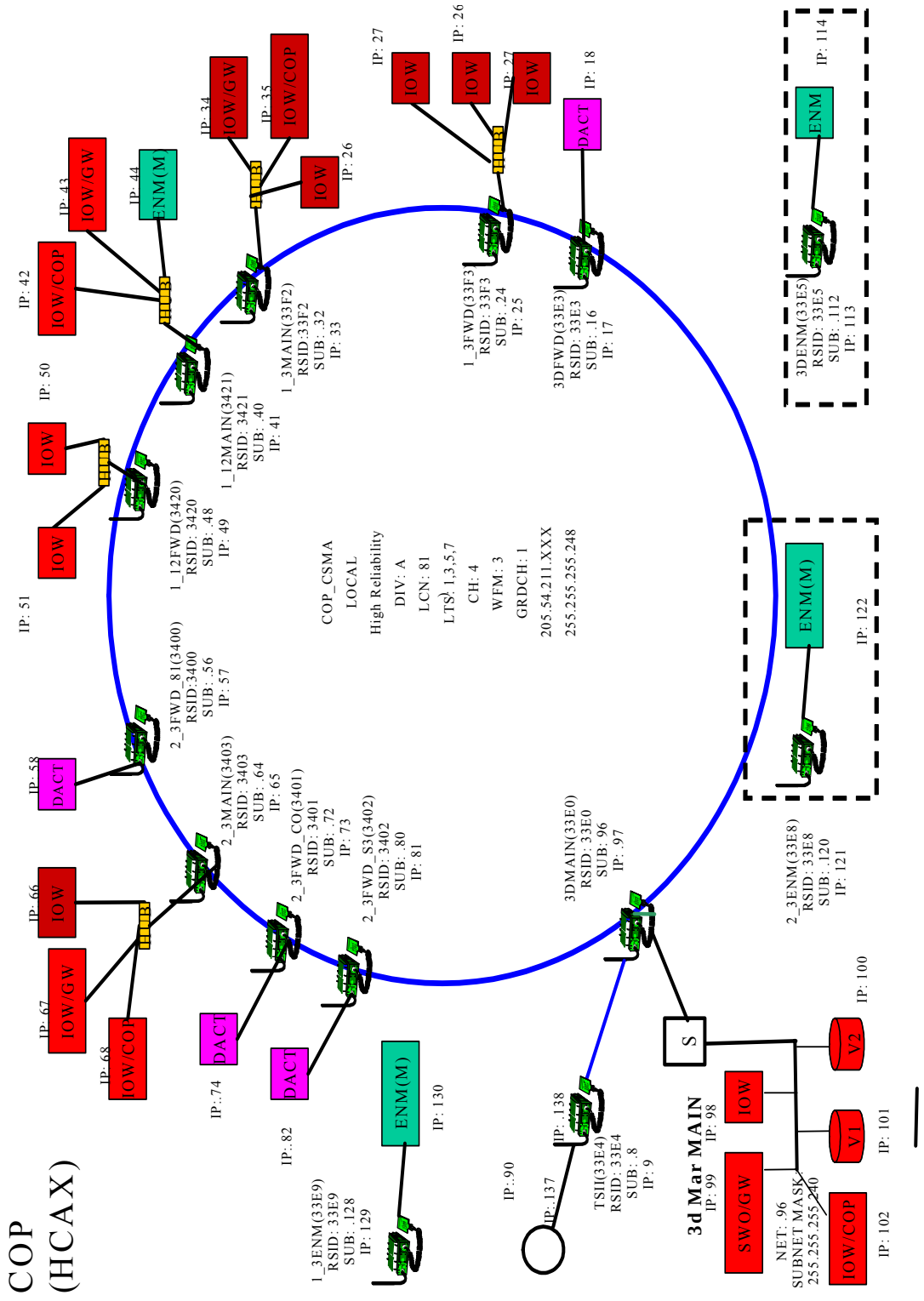

Figure 10. Sample EPLRS Network Diagram

EPLRS radios at the Infantry and Artillery Battalion would support one to three hosts per radio whereas the Regimental radios supported anywhere from one to nineteen hosts. Table 2 describes the type of hosts that used the EPLRS backbone.

EPLRS NETWORK	PURPOSE	HOSTS	PRIMARY APPLICATIONS	PRIMARY FUNCTION
C2	C2/CTP	IOS V1	S3 INFO SERVER	CTP DB HOST
		IOS V2	S2 INFO SERVER	MAPS, IMAGERY FILES
		ENM	C2PC 5.8.2 MS CHAT 2.0 MS OFFICE	CONTROLS EPLRS NETS
		IOS CLIENT		USER WORKSTATION
		IOW LAPTOPS		
		DACT		
FIRES	FSC	EMT		
		AFATDS	AFATDS	FIRE SUPPORT COORDINATION

Table 2. EPLRS Network Hosts and Applications [12]

The EPLRS network requires an EPLRS Network Manager (ENM) in order to design, initiate, and maintain the EPLRS network. Prior to deployment the ENM is used to configure an EPLRS network capable of supporting operational requirements. The ENM operator uses a Graphical User Interface (GUI) in order to define radios that will operate on the network, establish static routes, and assign channels to specific combat nets. During operations the ENM can either use one of the eight channels to support dynamic reconfiguration of radios or all eight channels can be assigned for use by combat nets. However, when all eight channels are assigned for use by supported combat nets the ENM can not reconfigure EPLRS radios or the EPLRS network.

The first ENM was mounted on the back of a five-ton truck; however, it was reduced in size to mount on the back of a HMMWV as shown in Figure 11 below. The latest iteration of the ENM is a ruggedized laptop with the ENM software program installed. (See Figure 12) The ENM offers increased capability yet significantly reduces the system footprint, taking the network management functionality from a HMMWV mounted system to a laptop.

Figure 11. Network Control Station (NCS)

Figure 12. ENM Version 10.X.

The Marine Corps procured 1187 EPLRS terminals, which are fielded to the Rifle Company and above. This system requires detailed planning prior to operations to ensure all communication terminals are properly configured, as well as a cadre of well trained communications personnel to install, operate and maintain them. Though EPLRS can be transported by footmobile units, it is typically mounted in a HMMWV. In short, EPLRS provides a dedicated, secure, mobile data communications network for MAGTF C4I users, delivering the data backbone for several Tactical Data Systems such as the Intelligence Operations Server (IOS), Intelligence Operations Workstation (IOW) and M-DACT/D-DACTs. EPLRS enables data exchange in unicast and multicast modes and is compatible with any terminal device (DACT, TCO, TDN server, and AFATDS) implementing the X.25 protocol. Within the Army and Marine Corps, EPLRS truly is the principal element of the digital backbone for ground forces.

d. Single Channel Ground and Airborne Radio System (SINCGARS)

Figure 13. AN/PRC-119 Manpack Variant of the SINCGARS Family

The SINCGARS family of tactical radios represents a technology developed in the early 1980s to serve as a replacement for the PRC-77, which was the tactical communications workhorse during the Vietnam conflict. The first major distribution of the SINCGARS radios was in 1990, and since that time, the radio which was originally a voice only system has undergone several key upgrades in order to increase performance as technology improves.

The SINCGARS family of tactical radios is used at every organizational level within the Marine Expeditionary Force: Division, Air Wing, and Force Service Support Group (FSSG) and is the primary means of on-the-move communications for command and control and fire support in the battlespace. A conservative estimate of the number fielded in the Marine Corps is approximately 22,000 units.

Several variants have been developed in order to meet existing communications requirements from the AN/PRC-119 (Pictured in Figure 13) dismounted short-range radio to the vehicular mounted long-range AN-MRC-145. Table 3 below briefly describes the different variants of the SINCGARS family of tactical radios.

Nomenclature	# of Radios	Amplifier	Description	Typical Range
AN/PRC-119	1 RT-1523	None	1 Dismounted short range radio	8 km
AN/VRC-87	1 RT-1523	None	1 Vehicle mounted short range radio	8 km
AN/VRC-88	1 RT-1523	None	1 Vehicle mounted short range radio configurable for dismounted operations	8 km
AN/VRC-89	2 RT-1523	1	1 Vehicle mounted long range radio 1 Vehicle mounted short range radio	RT with amplification: 35 km RT without amplification: 8 km
AN/VRC-90	1 RT-1523	1	1 Vehicle mounted long range radio	35 km
AN/VRC-91	2 RT-1523	1	1 Vehicle mounted long range radio 1 Vehicle mounted short range radio configurable for dismounted operations	RT with amplification: 35 km RT without amplification: 8 km
AN/VRC-92	2 RT-1523	2	2 Vehicle mounted long range radios	RTs with amplification: 35 km
AN/MRC-145	2 RT-1523	2	2 Vehicle mounted long range radios with a dedicated HMMWV	RTs with amplification: 35 km

Table 3. SINCGARS Family of Tactical Radios Adapted from [10]

The SINCGARS family of tactical radios is built around the receiver/transmitter (RT-1523) and interchangeable modular components such as the number of RTs, power amplifiers, vehicular mounts, and installation kits or manpack components. The addition of specific components to the basic RT determines the actual radio configuration and variant, as described in Table 3. The RT-1523 terminal operates in the Very High Frequency of 30 to 87.975 MHz. The power for this RT is variable from low to 50 watts with a power amplifier. Each system uses one of two omni-directional antennas, a three-foot tape, or a ten-foot collapsible whip antenna. Ranges for these radios vary from 300 meters to 35 Kilometers dependent upon power, antenna selection and placement, as well as line-of-sight considerations.

SINCGARS operates on any of 2,320 channels between 30 and 88 megahertz (MHz) with a channel separation of 25 kilohertz (KHz). [10] SINCGARS was designed for frequency hopping and comes with Frequency Hop (FH) mode in addition to integrated COMSEC (ICOM) features, which deliver robust Electronic Warfare (EW) capabilities, such as anti-jamming, low probability of detection (LPD), and low probability of intercept (LPI).

The most recent update to the SINCGARS family was the system improvement program (SIP) and the advanced system improvement program (ASIP). This added improved data transmission capabilities through a modem and implemented

the Reed-Solomon forward error correction (FEC) algorithm, as well as providing a smaller form factor. The SINCGARS ASIP, shown in Figure 13, is capable of 16 kbps under ideal conditions and limited distances.

SINCGARS has been used almost exclusively for voice communications until the recent fielding of the D-DACT, which uses a six-pin SINCGARS cable to connect to the AN/PRC-119 (manpack variant radio). The D-DACT uses a Taclink 3000 modem to transmit PLI data from the built in GPS receiver and Command and Control Compact Edition (C2CE) software over the SINCGARS Combat Radio Net. The D-DACT is discussed in greater detail in a subsequent section.

SINCGARS radios are the mainstay of mobile users, and in infantry units these radios are deployed down to the platoon. The Combat Radio Nets formed can be described as hierarchical in nature. For example, a Rifle Company will have its own radio net to which the Company Commander and each of his platoon commanders will subscribe. Each Battalion will have its own Battalion Tactical net (Bn Tac1) to which the Battalion Commander and each of his Company commanders will subscribe. Each Regiment and Division has its individual combat net that has designated units as subscribers. Of course, this is an over simplification but describes the basic formula.

A vast number of combat nets use SINCGARS radios spanning functions of command and control, fire support, administration and logistics, to name a few. Standard Operating Procedures (SOPs) as well as techniques, tactics and procedures (TTPs) have well established those nets that will be present in a tactical environment. Table 4 is a sample Radio Guard Chart for an Infantry Battalion and lists those nets that are commonly used.

CIRCUITS	SPMAGTF CTP	SPMAGTF FIRES	SPMAGTF CMD 1	SPMAGTF CMD 2	SPMAGTF TAC 1	SPMAGTF INTEL	SPMAGTF FSC 1	SPMAGTF FSC 2 DATA	SPMAGTF GRD REC	SPMAGTF COM COORD	BN TAC 1	BN TAC 2	ARTY COF 1	TACP LOCAL	STA CMD	81 COF	TAR / HR	TAD 1	ALPHA CO TAC	BRAVO CO TAC	CHARLIE CO TAC	CAAT TM 1	CAAT TM 2
EMISSION	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K	K		K	K	K	K	K	K
MODULATION	EPLRS	EPLRS	DAMA	HF	VHF	VHF	VHF	VHF	HF	VHF	VHF	VHF	VHF	VHF	VHF	VHF	HF	UHF	VHF	VHF	VHF	VHF	VHF
NET ID					000	001	002	003		000	001	002	003	004	005	006			000	001	002	003	004
RESTORATION PRIORITY	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
UNITS																							
SPMAGTF-X	C	C	C	C	C	C	C	C	C	C													
BN ***	X	X	X	X	X	X	X	X	X	X	C	C	X	C	C	C	X	X					
BN MAIN	X	X	X	X	X	X	X	X	X	X	X	X	X		X			X					
BN FWD	X	X			X		X				X	X	X		X			X					
STA TEAM 1											A	A			X								
TACP TEAM 1											A	A		X			X	X					
81's PLATOON											A	A				X							
ALPHA CO											X	A							C				
BRAVO CO											X	A								C			
CHARLIE CO											X	A									C		
CAAT TM 1											X	A										C	
CAAT TM 2											X	A											C
ARTILLERY BN							C	C		X	A		C										
CSSD-XX	X									X	A												
MAG-XX				A													A						
DASC										A							C	C					
HMH-XXX	X									A							A	W					
TECG	X									A													

LEGEND:
X-GUARD
C-NECOS
A-AS REQ
K-SECURED
W- WHEN DIRECTED
R-RETRANS

***-denotes in control of the battle

NETS
TAD 1
TAR / HR
SPMC-2
SPMGR
SQD COM

FREQ
xxx.xx
x.xxx
xx.xxxx
x.xxxx
xxx.xxx

UNITS
BN CO
BN XO
S-4 OFFICER
S-3 OFFICER
S-2 OFFICER
S-1 OFFICER
S-6 OFFICER
AIR OFFICER
FAC
ALPHA CO
BRAVO CO
CHARLIE CO
WPNS Co. CO
COLLECTIVE

CALLSIGNS

Table 4. Sample BN Radio Guard Chart

High-priority nets are run on high-power systems such as the AN/MRC-145 vehicle in order to benefit from power amplification and improved antennas, but clearly not every net can be run off these low density assets; therefore, net priority lists are prepared. Second-tier nets will be run off of OE-254 antenna masts, pictured in Figure 14, which raise the radiating elements of the antenna to a maximum height of 42 feet. Footmobile units will typically employ either three-foot tape or ten-foot whip antennas while on the move and will pause to use OE-254 antennas to improve connectivity to their desired station. The OE-254 antenna raises the ceramic radiating element to a height of 42 feet.

Figure 14. Two Marines Deploy an OE-254 Antenna

The SINCGARS family of tactical radios is indispensable to tactical operations because they provide secure wireless communications for small unit forces delivering robust EW capabilities and on-the-move communications. When fielded, these radios represented substantial enhancements over the gear they replaced, but today as the force becomes more agile, employing maneuver warfare to strike enemy centers of gravity and relying on increased situational awareness, these systems are stretched beyond their capacity.

These radios provide limited bandwidth to mobile units due to their origin as a voice only system, and require deliberate maneuver in order to maintain line of site between users. Ultimately the SINCGARS family of radios is scheduled for replacement by the Joint Tactical Radio System (JTRS) beginning with the vehicle mounted variant in FY 2008.

e. AN/PRC-150 High Frequency Manpack Radio (HFMR)

Figure 15. AN/PRC-150 High Frequency Manpack Radio (HFMR)

Fielded in 2001, the AN/PRC-150 as shown above in Figure 15, replaces the AN/PRC-104 HF radio. The PRC-150 represents significant improvements over the PRC-104 such as a built in encryption module, Automatic Link Establishment, and interoperability with existing VHF radios. The PRC-150 provides half duplex High Frequency (HF) and Very High Frequency (VHF) tactical radio communications from 2 to 60 MHz and is capable of long distance communications, approaching 30+ Miles. This radio supports voice or data (using a Modem) through Single Sideband modulation selectable for either Upper Side Band (USB) or Lower Side Band (LSB). The HFMR's 20-watt power output is provided by either battery or external electrical power. [10]

The dynamic environment and operations tempo of the modern battlefield causes mobile units to exceed the operating range of UHF and VHF radios routinely. The HFMR can maintain connectivity between physically separated units. The PRC-150 is commonly used by Reconnaissance Teams, Forward Air Controllers, and between maneuver units and higher headquarters. The HF link represented back in Figure 4 between Surveillance, Target Acquisition Team (STA Team) and Battalion Combat

Operations Center (COC) demonstrates a possible application of this radio. The PRC-150 is interoperable with the AN/PRC-104, AN/MRC-138, and Army/Navy HF ALE systems.

Use of HF radios is virtually an art, requiring a solid understanding of wave propagations, frequency selections, ionospheric conditions, and antenna construction. Consequently, proficient operators are becoming scarce. To use this radio effectively requires an operator with training notably beyond that required to operate SINCGARS.

f. AN/PRC-113 Ultra High Frequency Radio

Figure 16. AN/PRC-113 UHF Radio

The PRC-113 is a mainstay of Tactical Air Control Party (TACP) personnel. The UHF radio is a critical line-of-sight system almost exclusively used for ground-to-air coordination. Figure 4 shows a UHF link between operators at the battalion combat operations center (COC) and fixed-wing air assets overhead. This link could represent Tactical Air Direction Net (TAD 1). The PRC-113 operates in VHF from 116 to 150 MHz and UHF spectrum from 225 to 400 MHz. The AN/PRC-113, shown in Figure 16 above, is the manpack configuration of the receiver transmitter (RT)-1319 and requires two 12-volt lithium batteries. [10]

g. AN/PRC-148 Tactical Handheld Radio - (THHR)

Figure 17. AN/PRC-148 Tactical Handheld Radio (THHR)

The THHR was initially fielded in 2001 to provide a multi-band capability packaged in a small form factor for mobile users. The AN/PRC-148 shown in Figure 17 is interoperable with VHF and UHF radios between 30 and 512 MHz. The radio supports intra-team communications and links of greater range (up to 12 miles) through variable power levels. The user can select between .1, .5, 1, 3, and 5 watts to support mission specific requirements. The AN/PRC-148 is a system capable of providing small units (platoon, squad and fire team) embedded Type I communications security. The Marine Corps procured over 2,000 of these radios, and they are fielded down to the infantry company. [10]

The THHR is commonly used by platoon commanders to maintain voice communications with their respective squad leaders and because it supports UHF connectivity, TACP teams have also shown a strong interest in this radio. Figure 4 represents a VHF link between platoon commanders and their squad leaders that could be supported by the THHR.

h. Personal Role Radio

Figure 18. Personal Role Radio (PRR)

The Personal Role Radio, pictured in Figure 18, has recently been fielded to Marine forces in Iraq in very limited numbers; however, it has been widely distributed to 65,000 British armed forces. The Personal Role Radio operates in the 2.4 GHz ranges and uses a modified 802.11b protocol, which achieves transmission ranges of 500 meters in rural terrain and is touted as being capable of transmitting through three floors in an urban setting. The modulation scheme employed is Direct Sequence Spread Spectrum (DSSS) with voice coding (CVSD). The radio boasts compatibility with tactical HF, VHF, and UHF radios. The system comes with a wireless remote push-to-talk (PTT) device that operates at 433 MHz with a transmission range of about two meters. [13]

This system was the first tactical radio designed for distribution to every member of the unit and aims to eliminate the need for shouting to be heard over the din of battle. This system illustrates the direction small agile teams capable of independent action will require in order to fulfill the challenge and promise of Network Centric Warfare. Soon, each Marine will be a member of the network capable of both pushing and pulling relevant information up the chain of command.

i. Radio Systems Summary

The eight radios described in the preceding section represent a small portion of the entire C4ISR Architecture, accounting for eight out of 140 different assets detailed in the Marine Air Ground Task Force (MAGTF) C4IS Integrated Architecture Picture. However, these radios play an indispensable role in tactical connectivity for the Marine infantry regiment and below. The systems presented are mission specific and support specialized requirements, intended to disseminate information among pre-defined nodes and operators, but these rigid connections largely fail to support the needs of a network centric force. David Alberts, John Garstka, and Frederick Stein propose that Network Centric Warfare will increase combat power through the "networking (of) sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization." [2]

Today, valuable information originating from the fire team cannot autonomously traverse the systems described but instead, the information must be bridged by Marines at the seams. For example a fire team leader could contact his Squad Leader who has both a PRR and THHR. The squad leader would in turn relay the information to his Platoon Commander via the THHR. The platoon commander would bridge the traffic from his THHR to the Company Commander via his PRC-119, and this pattern would be repeated until relevant information was delivered to the Division. The same process in reverse is required for dissemination of information from higher headquarters. What is required are systems that are interoperable and create routable networks to leverage well established networking protocols.

2. Tactical Internet Nodes

In the beginning of the radio systems section, a model of mobility versus capability was discussed. Units that require a high degree of mobility to support their operations will use systems less capable than their counterparts which operate from more static positions. This hold true for Tactical Internet Nodes as well. Marines

throughout the MAGTF use computer systems to accomplish their assigned mission; however, the increased mobility and reduced footprint of small units demand different requirements from computing devices than higher headquarters.

This overview of MAGTF computing assets refers to the organizations structure from platoon to company and battalion and regiment and is based on Figure 19, which shows node connectivity. Figure 19 is referenced throughout this section to provide a visual model of asset distribution.

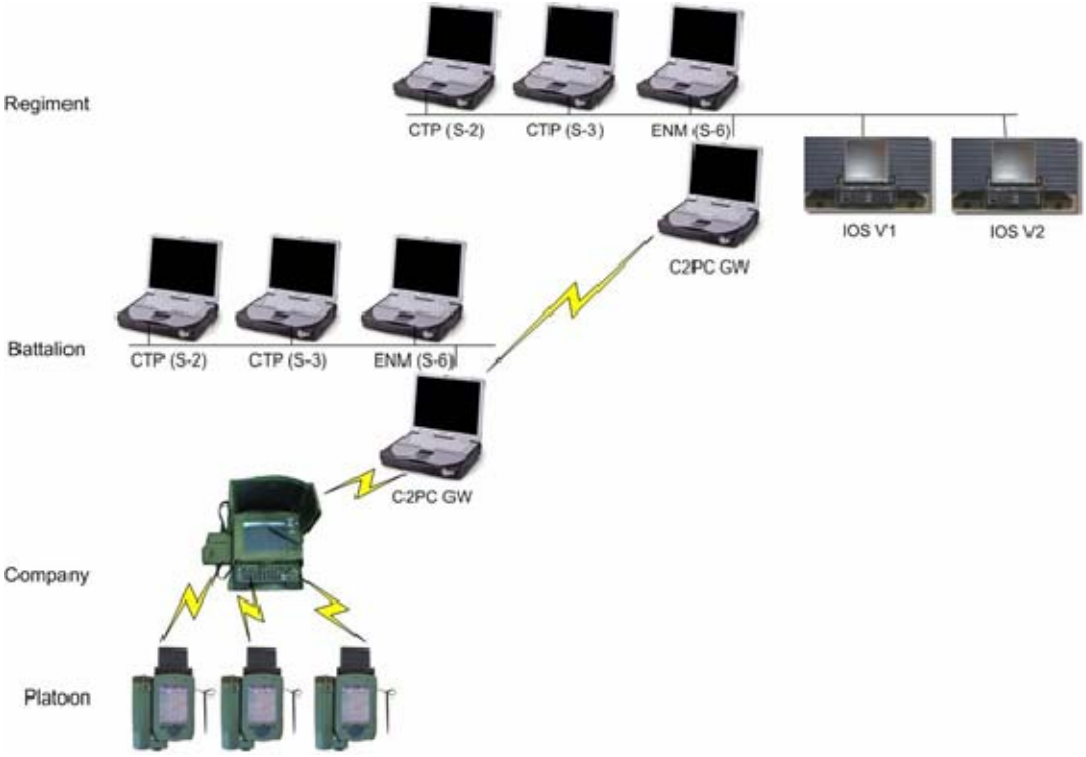

Figure 19. Command and Control Personal Computer Node Connectivity

In the previous section "Radio Systems," information was provided on the SCR systems that form the radio links to support the flow of voice and data across the battlespace. This section details several ruggedized computers, such as Intelligence Operations Workstations (IOWs), Intelligence Operations Servers (IOSs), Mounted Data Automated Communications Terminal, (M-DACT) and the Dismounted Data Automated Communications Terminal (D-DACT). These rugged systems are used by maneuver units in the most austere environments and are routinely subjected to dirt, dust, humidity,

and the extremes of hot and cold climates. The rate of technological advances dictates that the capabilities of these computing devices will continuously improve thus the data presented in this section "Tactical Internet Nodes" represents current information that is likely to become outdated as the systems undergo continuous improvement.

a. Dismounted Data Automated Communications Terminal (D-DACT)

Figure 20. Dismounted Data Automated Communications Terminal (D-DACT)

The Dismounted Data Automated Communications Terminal (D-DACT) (refer to Figure 20) is a rugged personal digital assistant (R-PDA) that delivers a unique set of features to improve the situational awareness of commanders at the Infantry platoon level and below. The D-DACT is a R-PDA-55 manufactured by Talla-Tech industries, designed around an HP Ipaq model 5550. It comes with an Intel 400 MHz X Scale processor and Windows Pocket PC 2003 operating system. The built-in memory consists of 128 MB of Synchronous Dynamic Random Access Memory (SDRAM) and 48 MB of flash Read Only Memory (ROM). The D-DACT comes with a 3.8" touch sensitive screen that works with an attached stylus. The D-DACT is fielded with a built-in Selective Availability Anti-Spoofing Module (SAASM) Global Positioning System (GPS) receiver and one PCMCIA slot. The system ships with a Taclink 3000 analog/digital modem manufactured by Raytheon and when coupled with the SINCGARS cable, this system allows for data transmission over the AN/PRC-119 and various other manpack radio systems. [14]

Situational awareness is enhanced through the automated transmission of Position Location Information (PLI) to the senior commander's Common Tactical Picture (CTP), as Figure 19 above illustrates. The D-DACT uses Command and Control Compact Edition (C2CE), the equivalent of C2PC software for systems using the Pocket PC operating system. C2CE delivers a view of the CTP to commanders at the platoon level and below. This capability greatly enhances their understanding of friendly and enemy positions, accelerating decision making and reducing the possibility of fratricide.

The D-DACT was designed for prolonged operations and comes with an external battery adaptor that can use either the BA-5800 lithium battery (originally designed for the AN/PSN-11 GPS receiver) or alkaline AA batteries. (Figure 21) Electronic transfer and storage of files is accomplished either through the use of SanDisk compact flash memory cards (Figure 22) or the proprietary serial cable. (Figure 23) Another key feature is the external GPS antenna port, which allows the operator to use the D-DACT while inside of a tactical vehicle, yet maintain a GPS signal. The operator simply connects an external GPS antenna to the D-DACT and places the external antenna on the outside of the vehicle. (Figure 24) The ability of the D-DACT to serve as a navigational aid even when not connected to a wireless radio network is a powerful capability that allows commanders to plan routes easily, to exchange those routes electronically, and to navigate with GPS-enabled precision.

Figure 21. Battery Adaptor

Figure 22. Memory Card

Figure 23. D-DACT Connected to Laptop via Serial Cable

Figure 24. D-DACT with External GPS Antenna

The sponsor of the system is the Project Management Office for Intelligence and Effects (PM IE), within the Army Program Executive Office for Command, Control and Communications Tactical at Fort Monmouth, NJ. The Army is using the R-PDA to implement Commander's Digital Assistant, which is similar in scope to the D-DACT program. [15]

The Marine Corps has procured over 600 D-DACTs and fielded the system to II MEF in Iraq in the spring of 2005. Initial user training went well and user input and feedback to support personnel from SPAWAR Center Charleston was very positive. Those who attended training routinely mentioned their desire to incorporate the D-DACT into convoy operations in order to aid navigation and to maintain situational awareness among vehicles and personnel in the convoy. A chat feature built-in to C2CE that allows users to type in free-text messages was viewed as a very useful communications tool by those attending training. (The C2CE application is presented in greater detail in subsequent section).

b. Mounted Data Automated Communications Terminal (M-DACT)

Figure 25. Mounted Data Automated Communications Terminal (M-DACT)

The M-DACT in Figure 25 is a rugged handheld computer (RHC), which in many ways mirrors the capabilities described above for the D-DACT. It is a laptop packaged for a rugged environment. The M-DACT program is more mature; Marine

Corps units received M-DACTs in fiscal year 2000. The M-DACT comes with an Intel 500 MHz processor and uses Windows NT 4.0 as its operating system. The built-in memory consists of 256 MB of RAM and a 30 GB hard drive. The RHC comes with a 6.4" touch sensitive screen and "QWERTY" keyboard. The M-DACT has built-in GPS receiver and one PCMCIA slot. The unit comes with a built-in Taclink 3000 analog/digital modem manufactured by Raytheon that allows the M-DACT to transmit data via the SINCGARS radios. [10]

The M-DACT comes loaded with C2PC and automates the transmission of PLI to the commander's Common Tactical Picture (CTP). The concept of employment for the M-DACT calls for it to serve as both a C2PC client and gateway. As represented in Figure 19, a Company Gateway will receive traffic from subordinate D-DACTs and correlate all the data for transmission to the battalion gateway (or senior gateway machine). The M-DACT will also run in client mode in order to allow the company commander to view the CTP.

The M-DACT was designed primarily for vehicular use and has been installed in HMMWVs, Amphibious Assault Vehicles (AAVs), M1A1 Abrams main battle tanks, and Light Armored Reconnaissance (LAR) vehicles, to name a few. The primary source of wireless radio connectivity is the EPLRS radio and the alternate is SINCGARS. When vehicle mounted, the M-DACT draws power from the host vehicle through installed cabling.

Figure 26. M-DACT Installed in a MRC-145 Vehicle

Figure 26 illustrates the installation of the M-DACT. At the infantry battalion level vehicular installation of the M-DACT generally includes the HMMWVs used by the Battalion Commander, Operations Officer, Fire Support Coordinator, and Combined Anti-Armor Teams (CAAT). To fully benefit from the M-DACT, these vehicles require the installation of EPLRS radio to provide wireless tactical radio connectivity. The installed C2PC software affords the operator a powerful suite of tools to support navigation, mapping, route and overlay creation, messaging, and improved situational awareness. (C2PC is covered in greater detail in a subsequent section). The Marine Corps procured over 600 M-DACTs, and the system is fielded down to company level.

c. Intelligence Operations Workstation (IOW)

Figure 27. Intelligence Operations Workstation (IOW)

The IOW pictured above in Figure 27, is a rugged commercial-off-the shelf laptop used by all echelons of command within the Marine Corps. These computers are used in austere environments not suited for standard computing devices. These rugged computers come with shock resistant magnesium alloy cases, moisture and dust-proof keyboards and touch pads, as well as gel or extra foam padding around the hard drive to provide protection from a fall of three feet onto concrete. Reports on these rugged laptops in Iraq are for the most part favorable, and one story reported by Christopher Allbritton borders on the miraculous. In his article "Birth of a Toughbook," July 13, 2004 edition of *Popular Mechanics* online, Allbritton tells the story of a US Soldier from the 82nd Airborne Division whose life was spared when the Panasonic Toughbook CF-34 laptop he was carrying stopped a bullet that had penetrated the HMMWV he was riding in. (See Figure 28).

Figure 28. Toughbook CF-34 Damaged by 7.62mm Projectile in Iraq [16]

The rate of technological advance dictates that the capabilities of these computing devices will continuously improve; therefore, the system capabilities presented here are subject to change. The Panasonic Toughbook CF-28 is one model used by operational units to support mobile computing requirements and comes with an Intel Pentium III 800 MHz processor and Windows XP Professional operating system. The CF-28 is powered by a lithium ion battery pack capable of four hours of continuous operation. The built-in memory consists of 256 MB of SDRAM and a 30-GB hard drive. The CF-28 comes with two PCMCIA slots and several interfaces to support 9-pin serial and 25-pin parallel connections as well as Universal Serial Bus (USB) and external keyboard/mouse.

Infantry battalions and regiments typically use their suite of IOWs inside the Combat Operations Center (COC), and provide a local area network (LAN) with Cat-5 cable, switches and routers. (Figure 29 below.) The systems are most often used by the Intelligence, and Operations Officers, and one may support the EPLRS ENM. These systems host the C2PC application and use EPLRS radio connectivity to gain access to command and control networks to deliver the CTP. The Marine Corps has procured over 500 of these systems, and they are fielded to all echelons of command.

Figure 29. Combat Operations Center at Headquarters Battalion of 1st Marine Division.

d. Intelligence Operations Server (IOS)

Figure 30. Intelligence Operations Server (IOS)

The IOS is a dual processor commercial-off-the shelf server packaged in a rugged transit case. The IOS system is a Sun Netra dual 400 MHz processor with 1 GB of RAM and two 36-GB hard drives. Two IOS systems are deployed at the regiment level; (reference Figure 30) IOS version 1 (V1) has the primary function of serving as the "operational planning tool for Marine Air Ground Task Force (MAGTF) commanders" and its "major functional capabilities include:

1. Maintenance and dissemination of a Common Tactical Picture (CTP)
2. Track management
3. Development and dissemination of operations orders and overlays."[17]

When the infantry regiment is operating with higher headquarters, the V1 server would access, retrieve, store, and present the relevant portion of the Global Command and Control System GCCS COP at Division.

The IOS (V2) has the primary function of providing "the automation of MAGTF intelligence activities, to include collection, processing and dissemination of multi-source, critical tactical intelligence" and its "major functional capabilities include:

1. All Source Intelligence Fusion at all command levels
2. Development of enemy ground situation
3. Access to Joint, Theater, and National intelligence
4. Rapid Tactical Intelligence production and dissemination." [17]

The Marine Corps has procured 200 IOS systems, and they are fielded to the infantry regiment and above.

e. Tactical Internet Node Summary

The four computer systems described in the preceding section play an indispensable role for operators throughout the various echelons of command. D-DACTs provide a mobile platform for commanders at the platoon level and below. M-DACTs offers mobile computing for primarily vehicular-mounted operations and are installed in HMMWVs, AAV, LARs and M1A1 main battle tanks. The M-DACT can serve as the gateway for D-DACT C2CE clients. IOWs are primarily used at the Combat Operations Center (COC) by intelligence and operations sections. IOWs routinely serve as C2PC gateways for M-DACT C2PC clients. Lastly the IOS systems version 1 and 2, supply secure storage of the COP and intelligence information. These systems represent a tiered system built to deliver reliable information up and down the chain of command and to operate efficiently in a distributed battlespace; however, they are often hampered by the limitations of the radio systems that provide wireless radio connectivity.

3. Tactical Internet Software Applications

In the Department of Defense (DoD) hundreds, if not thousands, of software applications are used every day to support a myriad of functional areas and requirements. Software applications assist in administrative, intelligence, operational, command and control, situational awareness, financial, and logistical domains to name a few. However,

concerning the tactical requirements of combat units at the regiment level and below, two applications stand out. The first and more mature application is Command and Control Personal Computer (C2PC) which is interoperable with the Global Command and Control System (GCCS). The second application is Command and Control Compact Edition (C2CE), which has only recently been distributed throughout the Marine Corps for use on mobile computing devices using the PocketPC operating system.

To become a proficient operator of C2PC and C2CE requires considerable practical application, far beyond the scope of this thesis. Therefore, this section offers the reader only a basic overview of these applications and highlights key features of the applications, such as mapping, overlays, signaling, and situational awareness, which are used in Chapter V Laboratory and Field Experimentation.

a. Command and Control Personal Computer (C2PC)

"Command and Control Personal Computer (C2PC) is a Windows-based client software application designed for Marine Air Ground Task Force (MAGTF) tactical data systems." [18] C2PC is installed on the M-DACT, IOW, and IOS computer systems described in Tactical Internet Nodes section of Chapter III. When C2PC is used over the tactical data network, it facilitates the exchange of position location information (PLI) data to generate a common operational picture (COP) of the battlespace.

In effect, C2PC provides the warfighter with a digital workspace that replaces paper map boards once prominently displayed in the Combat Operations Center (COC) of every echelon of command. Map boards of increasing complexity were required from platoon commanders and company commanders who may have maintained their own version on a foldable map. Battalion and regimental commanders used map boards similar to the sample shown in Figure 31 below. Paper-map boards required the use of acetate overlays to represent operational graphics and push pins to represent the position of units. Although these map boards were well integrated into standard operating procedures, a digital workspace has numerous advantages.

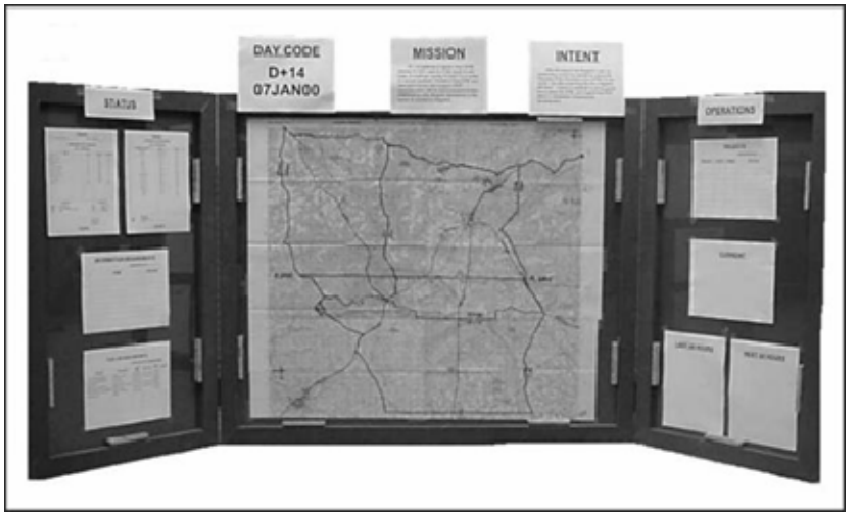

Figure 31. Example Paper Map Board

C2PC when operated over the tactical data network provides a means for commanders to maintain situational awareness akin to a paper-map board with greater efficiency. The emergence of the tactical Internet and data distribution on the battlefield is transforming the manner in which situational awareness is maintained. The overhead required to keep units updated on a paper map via combat radio nets and voice communications is significant. C2PC greatly reduces the amount of voice communications required to maintain situational awareness. Secondly, C2PC relieves the operators from constantly consulting their map, compass, and GPS receiver in order to track their position in the battlespace, as C2PC allows for GPS service and automatically transmits PLI data to other users on the network. These are only two examples of the benefits achieved through the use of a digital workspace like C2PC. The remainder of this section describes four features of the C2PC application: mapping, overlays, messaging and friendly and enemy situational awareness.

(1) Mapping. The mapping feature of C2PC provides a graphical representation of friendly and enemy units, overlays, and routes and allows Marines to visualize the battlespace. C2PC uses three primary sources of digital mapping information. The most commonly used is Compressed Arc Digitized Raster Graphics (CADRG). CADRG are traditional military paper maps that have digitized by an optical scanner. CADRG files are distributed either by Compact Disk (CD) or through the

Secure Internet Protocol Routable Network (SIPRNET). Figure 32 below shows a 1:25,000 scale CADRG map in use with the C2PC application.

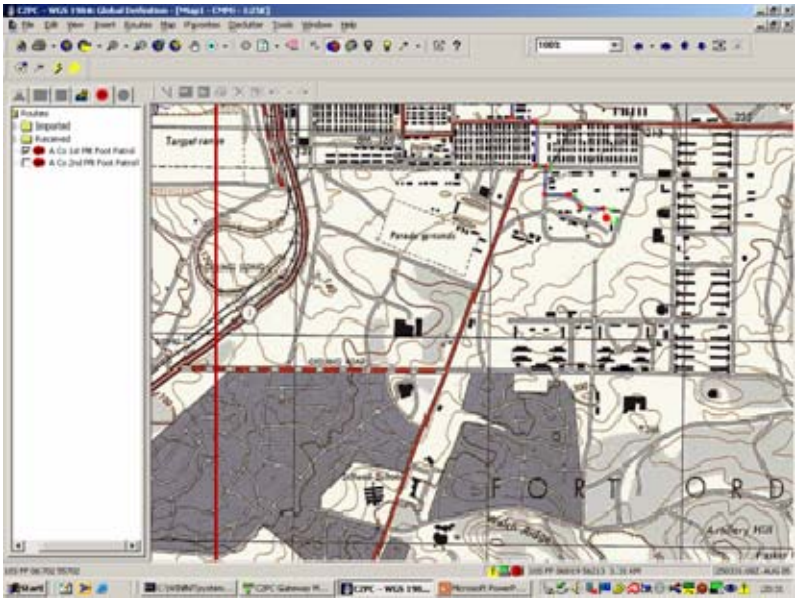

Figure 32. 1:25,000 Scale CADRG Map

The second type of mapping information used by C2PC is Digital Terrain Elevation Data (DTED). DTED provides elevation data that can be used for line-of-sight and to study the placement of weapons fans. The third type of mapping information used by C2PC is georeference imagery, which consists of Controlled Image Base (CIB) 5 (5-meter) resolution, CIB 1 (1-meter) resolution, and commercial satellite imagery. CIB 1 is particularly useful in urban areas. [19]

(2) Overlays. C2PC overlays can be used just as acetate was used in conjunction with paper maps. The operator can create the same symbols, lines, and circles that the Marine Corps used when creating overlays on acetate over paper maps. [14] Figure 33 shown below is a simple overlay created in less than five minutes. The benefit of digital overlays is that they can be transmitted electronically, printed, and reproduced in ways not possible with acetate overlays.

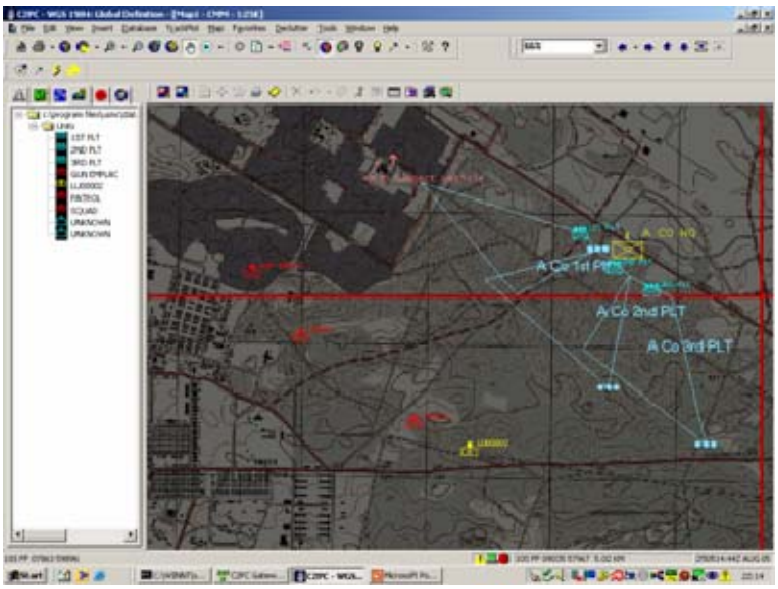

Figure 33. C2PC Overlay

(3) Messaging. The C2PC messaging feature was designed to support operators in transmitting preformatted and free-text message. The messaging application has several preformatted message types ranging from administrative, fire support, and logistics. The preformatted messages provide the user a template where specific information is either typed in or selected from a drop-down list. The free text message capability is provided by a Signal Composer dialog box. The Signal Composer keeps a log of all traffic that the user can scroll through. Figure 34 below shows text within the Signal Composer dialog box.

The messaging application also allows for distribution of overlays, routes, and electronic files (MS Word, MS PowerPoint, sound files, etc.). A user friendly Graphical User Interface (GUI) allows the C2PC operator to browse the system's hard drive, attach a file, and transmit it across the tactical Internet to the desired audience.

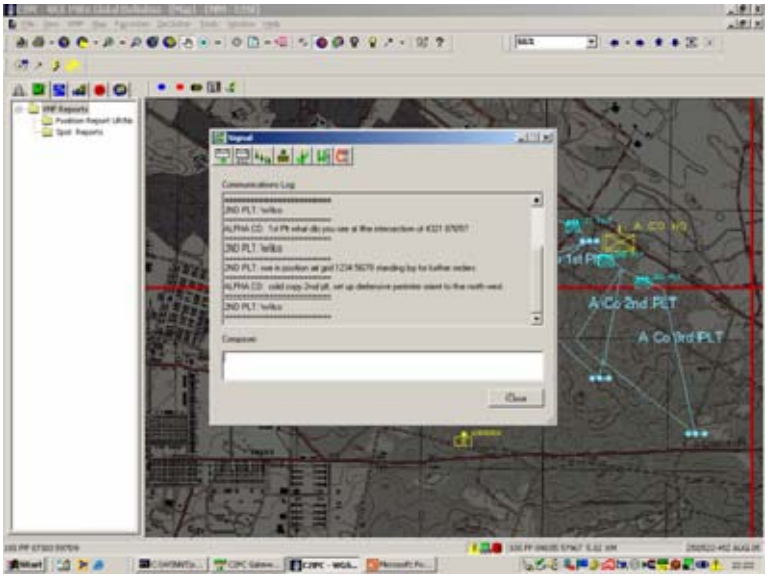

Figure 34. Signal Composer Dialog Box

(4) Friendly and Enemy Situational Awareness. Friendly and enemy situational awareness is supported through the dissemination of Tracks. "Tracks" is a generic name applied to digital icons that convey specific attributes about an object. For example a C2PC user could select an enemy track that would convey the unit size, activity, location, and the organization to which they belong, a time value such as when they were last observed, and the equipment they possess. That icon would then be represented on the C2PC digital workspace. Figure 35 shows sensor, friendly, enemy, and communications tracks deployed in Camp Roberts Military Installation.

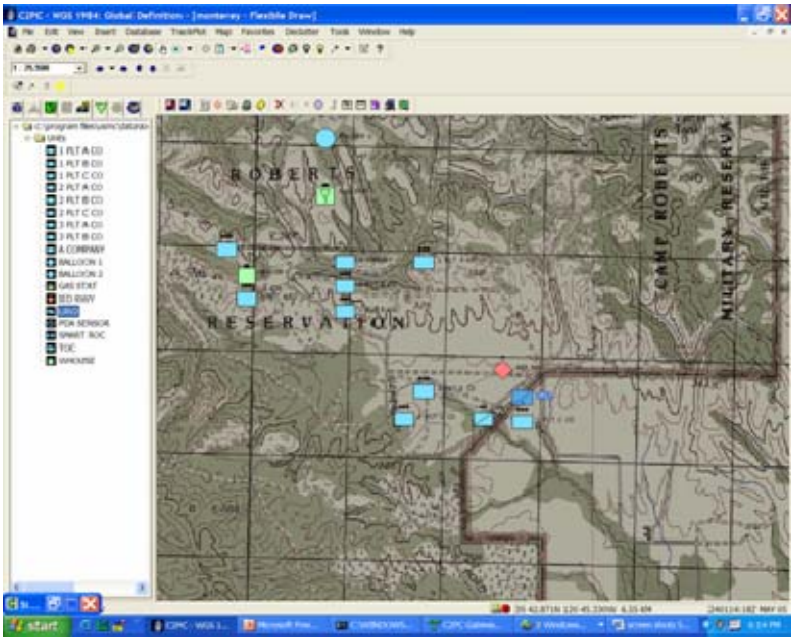

Figure 35. C2PC Sensor, Enemy and Friendly Tracks

The C2PC application is powerful because the features described above: mapping, messaging, overlays, and situational awareness can be shared across the battlefield over the tactical Internet. C2PC provides this functionality even when a node is in stand-alone mode, meaning the node is not currently connected to the network. When the stand-alone client rejoins the tactical network and reconnection to the Tactical Database Management (TDBM) server is re-established, track data will be synchronized.

Under the Family of Interoperable Operating Pictures initiative, C2PC is designated as the Joint Tactical COP Workstation, and the Marine Corps is the executive agent. Therefore, C2PC provides a single ground Blue Force tracking capability between the Marine Corps and the Army, and provides interoperability in the areas of intelligence, maneuver, logistics, fire support, and targeting between the Marine Corps, and the other services. [18]

b. Command and Control Compact Edition (C2CE)

Command and Control Compact Edition (C2CE) provides the functionality of C2PC for the PocketPC operating system used by the D-DACT. When C2CE is used over the tactical data network, it facilitates the exchange of position location information (PLI) data to generate a common operational picture (COP) of the battlespace. C2CE delivers the same suite of applications described in the C2PC section: mapping, overlays, signaling, and friendly and enemy situational awareness, but redesigns the functionality for the D-DACT platform.

Using the D-DACT requires the individual Marine to use a stylus to operate the PocketPC operating system, to use installed software application, and to enter data. The manipulation of a stylus on a hand-held computer is a challenge, particularly for Marines outfitted with their full combat load; however, clearly a great deal of consideration has been given to this crucial factor. Though mitigating all the inherent challenges of manipulating a stylus on a 3.8" screen is impossible, the design of C2CE prove to be user friendly from a usability perspective.

Captain Koichi Takagi, a 2005 graduate of the Naval Postgraduate School from the Operations Research department, performed a usability study on several models of mobile computing devices to include the D-DACT as part of his Masters of Science thesis, and his work is highly recommended for those interested in a more detailed analysis in this area. Captain Takagi's master thesis is titled "Applied Warfighter Ergonomics: A Research Method for Evaluating Military Individual Equipment."

(1) Mapping. The mapping application of C2CE supports the same digital mapping information described in the C2PC mapping section above: CADRG, DTED, and georeference imagery. One modification that has been made for the D-DACT is the ability to select an operational area for use as the background digital map. This modification was made in consideration of the reduced processing power of the D-DACT relative to M-DACTs, and IOWs. CADRG images are large files, in some instances as large as 70 MB; therefore, the D-DACT allows the operator to select only a

small portion of the entire CADRG map. This reduces the processing required when using the digital map. Figure 36 below shows the Operational Areas feature accessed from the map menu.

Figure 36. Operation Areas Are Accessed from the Map Menu

(2) Overlays. The C2CE overlay feature delivers an automated means to create the digital equivalent of acetate overlays used in conjunction with paper maps. The operator can create the same symbols, lines, and circles that the Marine Corps use when creating overlays on acetate over paper maps. The functionality provided here is consistent with that provided in C2PC. Figure 37 below shows the C2CE representation of the same overlay, as in Figure 33 in the C2PC overlay section. This overlay was produced in less than five minutes on an IOW using C2PC and transmitted over SecNet-11 SWLAN.

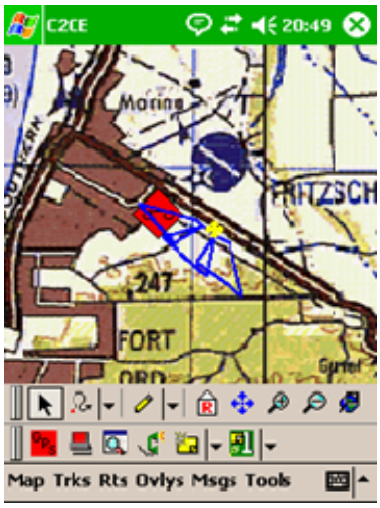

Figure 37. C2CE Overlay

(3) Messaging. The C2CE messaging feature allows operators to prepare and transmit preformatted and free-text messages readily. The C2CE messaging application has twelve preformatted message types ranging from a Nuclear Biological Chemical (NBC) report to a Call for Fire. The preformatted messages provide the user a template where specific information is either typed in or selected from a drop-down list. Figure 38 below shows the list of preformatted messages the operator can select.

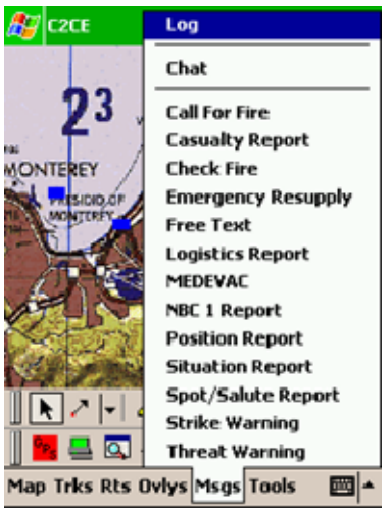

Figure 38. C2CE Preformatted Messages

The free-text message capability is provided by a Signal Composer dialog box. The Signal Composer keeps a log of all traffic, which the user can scroll through. The messaging application also allows for the electronic file transfer of overlays, routes, and electronic files (MS Word, MS PowerPoint, sound files, etc.). A user friendly Graphical User Interface (GUI) allows the C2CE operator to browse the system's hard drive, attach a file, and transmit it across the tactical Internet to the desired audience. Delivery confirmation receipts are also generated for assurance that the messages were received. Figure 39 shows a pop-up box on the screen of a D-DACT alerting the user that a route plan has been received from the Alpha Company commander.

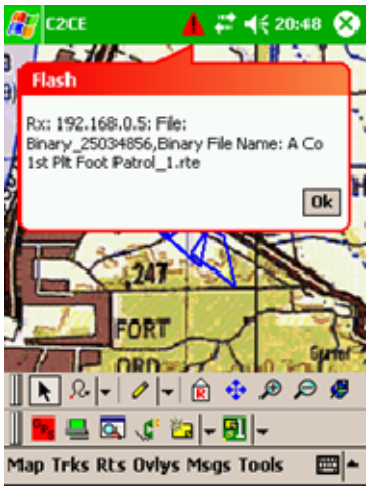

Figure 39. C2CE File Receipt Alert

(4) Friendly and Enemy Situational Awareness. Enemy and friendly situational awareness is supported by creating, inserting, and disseminating Tracks in the C2CE digital workspace. Tracks manually inserted into C2CE are forwarded to the C2PC gateway. D-DACTs at the platoon level would connect to their respective company C2PC gateway, which in turn would forward all Tracks to the Battalion gateway. (Reference Figure 19 in the Tactical Internet Nodes section to review C2CE and C2PC connectivity.) PLI data is automatically transmitted to the C2PC gateway when the D-DACT is connected to the tactical Internet. Figure 40 below shows enemy and friendly tracks displayed on the D-DACT screen.

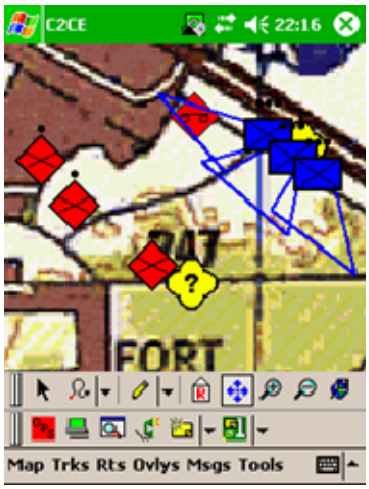

Figure 40. C2CE Friendly and Enemy Tracks

c. Tactical Internet Software Applications Summary

This section briefly summarized the C2PC and C2CE applications in order to introduce these powerful tools and to highlight key functions that resurface in Chapter V "Laboratory and Field Experimentation." These applications are robust programs that offer far greater utility than presented here.

B. TACTICAL INTERNET SUMMARY

This chapter covered the communications assets, computer terminals, and software applications that together form the tactical Internet. All elements of the MAGTF rely on these systems for command and control and to establish and maintain better situational awareness. However, these systems were designed to support voice traffic and subsequently evolved to meet service and application specific requirements. These systems have evolved as technology advanced; however, their underpinnings as voice assets limit their ability to internetwork. The specialization of these radios has created an environment of point-to-point links that are highly inflexible.

The characteristics of these radio systems fail to support the requirements of a network centric force that require real-time information from networked sensors, collaborative systems, and input from decision makers across the battlespace. Therefore, the challenge is to develop the network that will support network centric operations and

provide our forces greater lethality, increased survivability, and a greater degree of self-synchronization.

IV. LEVERAGING IEEE 802.11B AND 802.16 WIRELESS TECHNOLOGIES

A. BACKGROUND

The interest to experiment with the D-DACT, IEEE 802.11b and IEEE 802.16 wireless technologies was ignited through work with the Tactical Network Topology (TNT) Field Experiments at the Naval Postgraduate School. TNT experiments take place quarterly at Camp Roberts Army National Guard Base, near Paso Robles, CA, through a sponsorship with Special Operations Command (SOCOM). The experiments are a test vehicle for new technologies and investigate how new technologies can be leveraged to support the warfighter.

The TNT experiments provided exposure to ongoing work with mobile computing devices leveraging IEEE 802.11b wireless technologies. Of particular interest was the rugged personal digital assistant (R-PDA) manufactured by Inter-4. The R-PDA was integrated into the experiments and used by Special Operations Force (SOF) personnel to send small unit information to their headquarters in Tampa, Florida. The operators were using a Tacticomp with a built-in IEEE 802.11b wireless card, shown in Figure 41 below. This was used to join an ad-hoc local area network that was bridged onto an IEEE 802.16 radio wide area network (WAN), with a connection to a point of presence (POP) to the Internet. After viewing the Tacticomp in action, the Marine Corps' R-PDA, the D-DACT was implemented into similar experiments at Camp Roberts, CA.

Figure 41. Tacticomp

It became evident that the technologies employed by the Tacticomp could be leveraged by the D-DACT program with certain modifications. The Tacticomp used a COTS IEEE 802.11b wireless card for communications. This commercial card was ideal for initial experiments to demonstrate proof of concept for the technology, but its inherent security weaknesses needed to be addressed in order to be useful to Marine Corps operators.

There are numerous documented weaknesses associated with either Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) and both fail to provide sufficient protection for the confidentiality, integrity or availability of wireless traffic. The devices relying on WEP or WPA for protection in a WLAN are not authorized for operation in DoD networks. The Marine Corps has directed that at a minimum Federal Information Processing Standard (FIPS) 140-2 certified devices are required for UNCLASSIFIED wireless networks. [20] SECRET networks require the use of NSA Type 1 encryption devices. [21]

One possible alternative was the Harris SecNet-11 secure wireless Local Area Network (SWLAN) personal computer (PC) card. From there sprang the desire to integrate the SecNet-11 PC card into the D-DACT to provide a SWLAN that could be backhauled through an 802.16 WAN to an Internet POP.

This chapter will provide an overview of the wireless technologies, network protocol analyzers, and equipment tested during TNT field experiments and in the laboratory, which could provide a secure wireless routable network for the D-DACT. The intent of this overview is not to explicate any specific technology in detail, but instead to provide an appreciation for the technologies used in Chapter V Laboratory and Field Experimentation.

B. HARRIS CORPORATION'S IEEE 802.11B BASED SECNET-11 PRODUCTS

Harris Corporation's SecNet-11 line of products is the only wireless local area network technology to receive the National Security Agency's (NSA) certification for Type 1 encryption. SecNet-11 devices provide encryption at the data link layer and should be employed as part of DoD's "Defense in Depth" to ensure the confidentiality, integrity, authenticity, traffic analysis, and availability of data on the wireless network. SecNet-11 products are authorized to transmit information up to the SECRET level and operate on a wide variety of computing platforms. SecNet-11, being layer one, requires that all nodes within the network run at a single system high level of classification. Without re-keying and cleansing, it cannot run at any other level. SecNet-11 supports the following Microsoft Windows operating systems: Windows NT 4.0, Windows 98, Windows 2000, Windows ME, Windows XP, PocketPC 2002 and PocketPC 2003, as well as the Linux operating system.

The SecNet-11 PC card is a Personal Computer Memory Card International Association (PCMCIA) card (see Figure 42 below) that operates in the 2.4 GHz Instrumentation Science and Medical (ISM) band in accordance with the IEEE 802.11b protocol using Direct Sequence Spread Spectrum (DSSS) modified to allow for encryption delays.

Figure 42. Harris SecNet-11 PC Card

DSSS can achieve data rates of 1, 2, 5.5, and 11 Mbps. These rates are supported by the use of fourteen channels in the ISM band, eleven of which are authorized for use in the United States. These eleven channels are identified simply as channels 1 through 11. Each channel is centered on a specific frequency. For example channel 1 is centered on 2412 MHz and channel 3 is centered on 2422 MHz. [22] Due to channel spacing, there is overlap between the channels in the ISM band. It is recommended to use only three channels simultaneously in a collocated environment to reduce possible interference. Figure 43 below shows the 802.11b High Rate (HR) DSSS channels authorized for use in the US. Channels one, six, and eleven allow for the least interference when operating in a collocated environment.

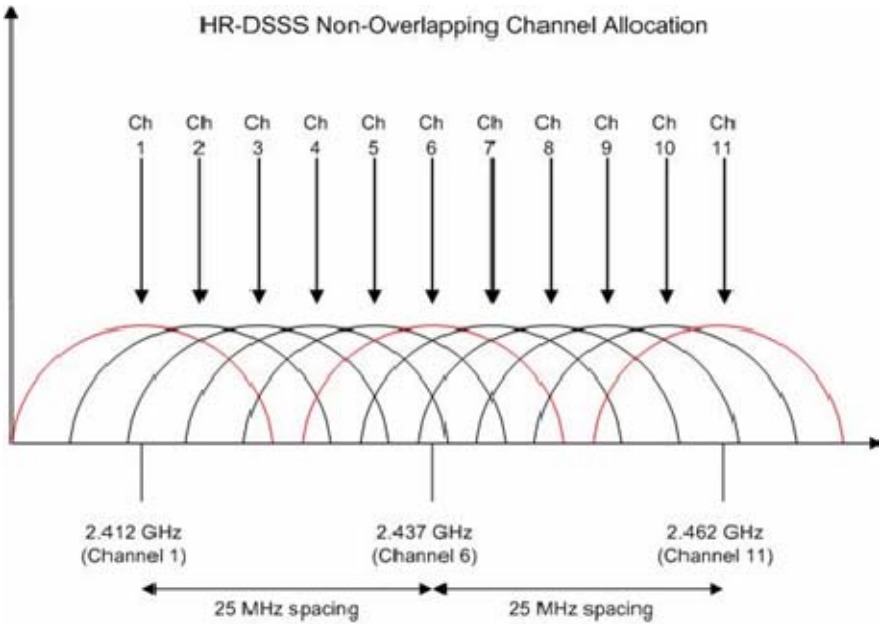

Figure 43. 802.11b Non-Overlapping Channel Allocation Adapted from Reference [22]

A shared wireless media is subject to the restriction that only one station can transmit at a time within a given channel. Therefore the IEEE 802.11b protocol specifies the use of the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) arbitration scheme. CSMA/CA is implemented through two primary measures: a clear-channel assessment (CCA) and the virtual carrier sense assessment. Both the CCA and the virtual carrier sense must report that the medium is idle in order for the node to transmit. If either the CCA or the virtual carrier sense report the medium is busy, then the node must defer until the medium is idle.

The SecNet-11 product line includes the PC card described above, as well as wireless access points (APs). Most commercial APs can be operated in three modes of operation: root, bridge, and repeater mode. None of these modes are defined in the IEEE 802.11b protocol, but root mode best describes the default configuration of most APs. The three operational modes of access points will be covered briefly because the experiments performed in this thesis used the Ad-Hoc functionality of the SecNet-11 card instead of the Infrastructure mode generally provided by access points.

When in root mode, the AP is generally connected to a distribution system by its wired interface (typically Ethernet). When operating in root mode, access points that are connected to the same wired network can talk to each other over the wired segment. These APs allow for associated stations from one AP to communicate with associated stations from another AP. Figure 44 shown below, demonstrates a distribution system with two APs in root mode. The APs each have three associated clients, which together comprise the Basis Service Set (BSS).

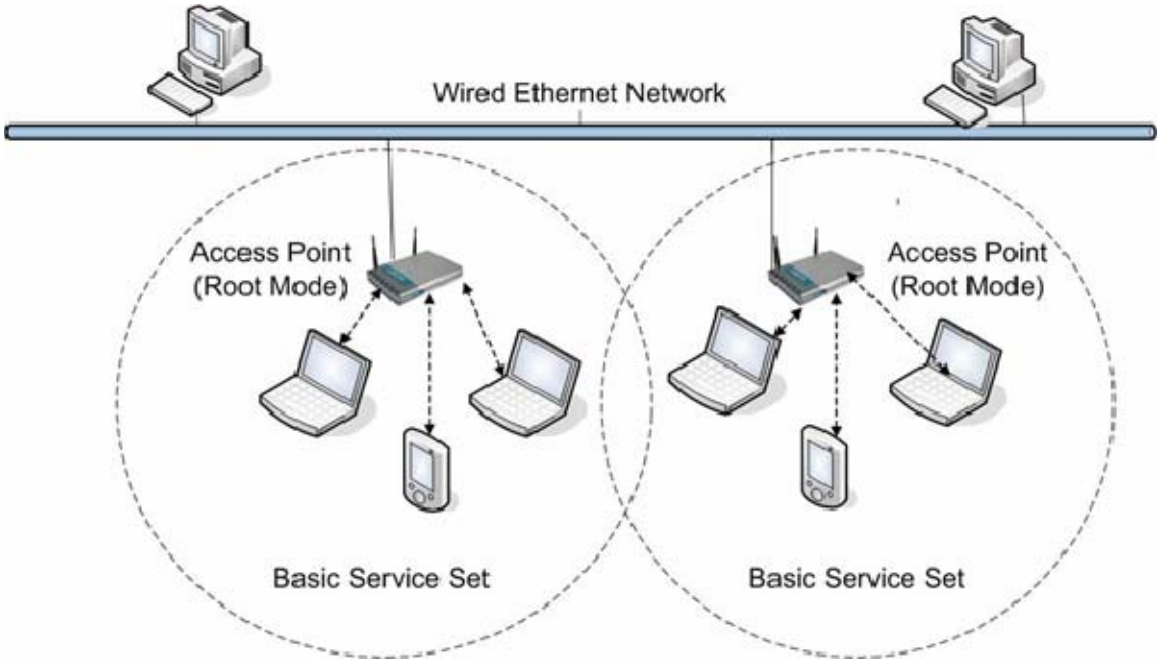

Figure 44. Distribution System with AP in Root Mode

Bridge mode creates a wireless distribution link between two (point-to-point) or more (point-to-multipoint) access points. In bridge mode, APs associate with each other but disallow associations from wireless stations. Repeater mode allows for an AP to provide intermediate connectivity between a root AP and clients that are out of range of the root AP. [22]

An independent basic service set (IBSS) is used to create an ad hoc network and consists of one or more 802.11b stations that are within mutual communication range of each other. Every station in the IBSS must be able to "hear" every other station in the

IBSS since there is no access point to forward frames between stations. Each station must be able to transmit data directly to every other station in the IBSS. [22] Ad-hoc networks, also known as peer-to-peer networks, are typically established for short periods of time and are the easiest wireless networks to implement. All SecNet-11 devices, which have the same service set identifier (SSID), are configured to use the same channel and have the same communications security (COMSEC) keying material can participate in the ad-hoc network. Figure 45 below shows a simple ad-hoc network.

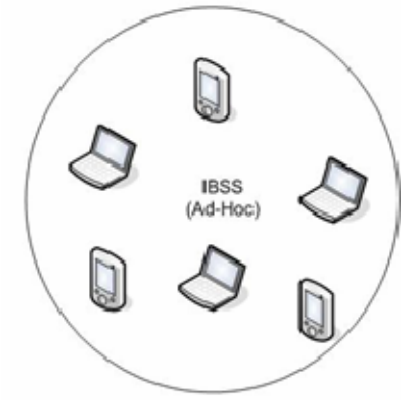

Figure 45. Ad-Hoc Network

The SecNet-11 products use Communications Security (COMSEC) to protect the entire IEEE 802.11b media access control (MAC) protocol data unit (MPDU). The SecNet-11 card receives keying material through a proprietary key fill cable that attaches at one end to the PC card and on the other to an AN/CYZ-10 data transfer device (DTD). Once the PC card receives keying material it becomes classified at the same level as the keying material. Figure 46 below shows a DTD connected to the SecNet-11 PC card.

Figure 46. AN/CYZ-10 Data Transfer Device Connected to SecNet-11 PC Card

The SecNet-11 PC card is an extended length PCMCIA card that is approximately two-inches longer than the typical commercial-off-the-shelf (COTS) PC card. The length of the PC card required that the plastic protective dome on the D-DACT be removed. Removing the protective dome disabled the built-in GPS antenna requiring the use of an external GPS antenna to provide reception from overhead satellites. Figure 47 below shows the D-DACT with the protective dome removed and the SecNet-11 PC card inserted.

Figure 47. D-DACT with Protective Dome Removed and SecNet-11 Card Inserted

The SecNet-11 PC card has two female SMA connectors on the face of the card, which provide dual antennas for spatial diversity. External antennas are connected to the

SMA connectors, and the SecNet-11 PC card typically ships from the manufacturer with two dipole antennas, which have an antenna gain of 2dBi. The SecNet-11 PC card has a transmit power specification of 39.8 mW when set to high power and 12.6 mW in the low-power setting. Figure 48 below shows the SecNet-11 PC card with antennas removed in order to view the female SMA connectors.

Figure 48. SecNet-11 PC Card with Two SMA Connectors

To confirm the specified transmission power of theSecNet-11 PC card, CenGen performed SecNet-11 PCMCIA power output measurements in December 2002. The results were described in Secure Wireless Networking: SecNet-11 Testing, by Steven Durbano and Joe Matkowski. The report was produced for the Office of Naval Research (ONR) as part of ongoing work on The Littoral Combat and Power Projection Future Naval Capability project.

CenGen used fifty SecNet-11 cards during their experiment in order to obtain a reliable sample. Four tests were run per card, to test the power output of Antenna A and Antenna B of the SecNet-11 card in both high and low transmit power. The tests were performed by placing the SecNet-11 card in the PCMCIA slot of a computer and connecting the desired SMA antenna connector to a power meter. The card listed as number nine in the table below was found to be defective, therefore, “not applicable” (N/A) is entered as a value for card nine. The values for cards one to fifty are provided in

Table 5 below. Also available is the high and low value, the average and three times the standard deviation for each or the four tests. Harris' specifications are provided at the bottom of the table.

Results	Antenna A High Power (dBm)	Antenna A Low Power (dBm)	Antenna B High Power (dBm)	Antenna B Low Power (dBm)
Card 1	17.75	10.45	17.05	10.45
Card 2	17.75	10.45	18.05	10.55
Card 3	16.80	10.30	17.30	10.50
Card 4	17.15	11.15	17.55	11.35
Card 5	16.80	9.70	16.20	9.20
Card 6	16.50	9.80	16.40	9.20
Card 7	16.90	10.20	18.20	9.80
Card 8	17.10	10.40	16.30	10.40
Card 9	N/A	N/A	N/A	N/A
Card 10	17.05	10.85	17.05	10.15
Card 11	17.35	11.05	17.65	10.45
Card 12	17.40	10.80	16.60	9.80
Card 13	17.45	11.05	16.95	10.65
Card 14	18.15	11.95	17.85	11.55
Card 15	17.75	11.45	17.75	11.35
Card 16	17.35	10.35	17.35	10.55
Card 17	16.50	9.80	16.30	9.10
Card 18	17.50	10.70	17.40	10.70
Card 19	17.50	10.20	17.20	10.20
Card 20	16.75	9.45	16.45	9.55
Card 21	16.75	11.05	17.05	10.65
Card 22	17.45	9.80	16.95	9.85
Card 23	16.95	10.05	16.05	10.25
Card 24	17.55	10.45	17.05	10.35
Card 25	17.15	10.95	17.55	10.95
Card 26	17.20	10.40	17.90	10.90
Card 27	16.40	10.40	16.90	10.80
Card 28	16.95	11.05	16.55	10.35
Card 29	17.65	11.15	17.75	11.45
Card 30	17.55	11.45	17.45	11.55
Card 31	17.06	10.75	17.05	10.55
Card 32	17.15	10.75	16.65	9.75
Card 33	16.70	10.50	17.20	10.50
Card 34	16.80	10.40	17.50	10.70
Card 35	17.55	11.05	17.75	11.45
Card 36	17.05	9.95	17.05	10.05
Card 37	17.20	10.40	17.80	10.60
Card 38	16.80	10.20	16.30	9.20
Card 39	17.20	9.50	16.20	9.60
Card 40	17.05	10.95	17.45	11.25

Card 41	16.80	9.60	16.70	10.80
Card 42	17.65	9.95	17.05	10.05
Card 43	17.30	9.70	16.80	9.10
Card 44	17.75	11.35	17.65	11.45
Card 45	18.10	11.20	16.60	10.80
Card 46	17.15	10.85	16.85	11.15
Card 47	17.30	10.20	16.80	9.80
Card 48	17.15	10.55	16.65	10.05
Card 49	16.95	10.65	17.05	10.75
Card 50	16.65	11.45	16.45	10.35
Low Value	16.40	9.45	16.05	9.10
High Value	18.15	11.95	18.20	11.55
Average	17.19	10.55	17.07	10.42
3σ (3 X Standard Deviation)	1.21	1.74	1.64	2.03
Harris SecNet-11 PCMCIA Card Specified Output Power Values				
Specification	16.00	11.00	16.00	11.00
3σ (3 X Standard Deviation)	± 2.00	± 2.00	± 2.00	± 2.00

Table 5. SecNet-11 PCMCIA Power Output Measurements [23]

The power output tests performed by CenGen indicate that the power output measurements in the high-power setting exceed the manufacturer's specifications. For Antenna A in the high-power setting, the average was 17.19 dBm with a standard deviation of ± 1.21. The power output specification Harris designed was 16 dBm with a standard deviation of ± of 2.00. Antenna B in the high-power setting had an average of 17.07 dBm with a standard deviation of ± 1.64. The power output of both Antenna A and B was within Harris' specifications when using the low-power setting.

An understanding of the output power for an 802.11b wireless device, as well as the antenna gain of the device, is crucial in estimating the range these systems can support. 802.11b receivers must receive sufficient signal strength from an access point or from another 802.11b transmitter in order to process the information being sent. A conservative estimate is that the receiver should have "receive signal strength" of at least -70 dBm. Typical 802.11b wireless devices can support ranges of approximately 300 meters. This approximate range is calculated using the Free Space Path Loss (FSPL) equation.

Path Loss(dB) =20*Log10[(4*π*D)/λ]

D= distance (in like units as λ)

λ= wavelength calculated as c/f (C=speed of light f=frequency).

Using the path loss equation, for a distance of 300 meters, and a frequency of 2,412 MHz returns a loss of 89.63 dB. This means that over a span of 300 meters a wireless device transmitting at 2412 MHz will lose 89.63 dB due to FSPL. To complete this example, use the attributes provided in Table 6 below.

Transmit Power	+16 dBm
Transmitter Antenna Gain	+2 dBi
Transmitter Connector Loss	+0
Path Loss	-89.63 dBm
Receiver Antenna Gain	+2 dBi
Receiver Connector Loss	+0
	-69.63 dBm
Required Signal Strength	-70 dBm

Table 6. 802.11b Range Example

In this example, the transmitting station has a power output of 16 dBm, no cable or antenna connector loss, and 2 dBi of gain from its antenna. The receiving station has 2 dBi of gain from its antenna and no cable or antenna connector loss. The power received at the receiving station is -69.63. Given that the received signal strength level was estimated at -70dBm, a range of 300 meters is theoretically supportable. This presumes clear line of sight and an electromagnetic noise-free environment.

Wireless devices with operating ranges of 300 meters can support various applications: commercial users who deploy wireless systems in a corporate environment and private users who deploy wireless systems in their homes, but generally this is insufficient for highly mobile users operating in a tactical environment. This challenge led to the implementation of Optimized Link State Routing (OLSR) to help mitigate the inherent short-range characteristics of 802.11b devices.

C. MOBILE AD-HOC NETWORKING (MANET)

MANET nodes can move arbitrarily; therefore, the network that supports them must be self-adapting to the connectivity and propagation conditions, as well as to the traffic and user mobility pattern. Each node in a MANET network will logically consist of a router with one or more hosts, and communications devices.

The MANET network is capable of functioning as a stand-alone network, but this delivers limited functionality. A more robust MANET network can be globally connected through an Internet point of presence (POP) accessible through one or more fixed networks. [24] Three classifications of MANET routing protocols exist: proactive, reactive, and hybrid, which are being standardized by the Internet Engineering Task Force (IETF). Each approach has advantages and disadvantages that must be considered for the intended application.

1. Proactive MANET Protocols

Proactive MANET protocols such as OLSR and destination-sequenced distance vector routing (DSDV) are table-driven and use stored values to maintain a record of routes to nodes on the network. This approach reduces the latency of data delivery since the route is stored and immediately available when required. The drawback is that this approach incurs a communications overhead required to maintain link tables for all routes in the network.

2. Reactive MANET Protocols

Reactive MANET protocols such as ad-hoc on-demand distance vector routing (AODV) and dynamic source routing (DSR) determine routes between nodes on demand. This means that a route for the delivery of information is not selected until a node on the network has information to transmit. This approach reduces the communications overhead required of the table-driven proactive approach, but could mean route information will not be available when a route request is received. This could lead to a delay between route request and transmission as the optimal route is being determined.

3. Hybrid MANET Protocols

Hybrid MANET protocols exhibit reactive and proactive behavior. One implementation is zone routing protocol (ZRP). This approach uses a proactive table-

driven approach within a restricted geographic area and determines routes on demand if a packet needs to traverse several of these zones.

4. Optimized Link State Routing (OLSR)

Optimized Link State Routing (OLSR) is one of several mob MANET protocols developed to meet the needs of mobile clients.

The key features of OLSR are

1. OLSR uses hop-by-hop routing, meaning that each node uses its local information in order to route packets to the next hop.
2. OLSR minimizes the overhead associated with flooding of packets on a network through the use of multipoint relays (MPRs). Only MPRs transmit control traffic in an OLSR network.
3. OLSR determines the optimal route in terms of the number of hops a packet will need to complete in order to reach its ultimate destination.
4. OLSR is designed to work in a completely distributed manner; therefore, it does not require a central entity such as an access point.
5. OLSR does not require the sequenced delivery of messages. Each control message contains a sequence number that is incremented for each message. This allows the recipient to assemble each message that has been reordered in transmission.
6. OLSR supports any existing IP stack because it only interacts with the routing table management. OLSR does not require changes to the format of IP stacks.
7. OLSR creates a UDP datagram to encapsulate packets for transmission over the OLSR network using port 698. [25]

The central concept used in the OLSR protocol is the use of multipoint relays (MPRs). These are nodes that are selected by computer terminals in the network that are responsible for forwarding broadcast messages during the flooding process. Delivery of control messages to all the nodes in a network used the concept of flooding. However,

traditional schemes accomplished this by requiring every node on the network to rebroadcast each control message it received to every destination with whom the receiving terminal had communications. That process is illustrated in Figure 49 below. The use of a sequence number prevents loops; therefore, each receiving station only transmits the message once. As Figure 49 illustrates, this method requires N-1 retransmissions where *N* is the number of nodes in the network. In this example there are 25 nodes, therefore, the datagram would be retransmitted 24 times.

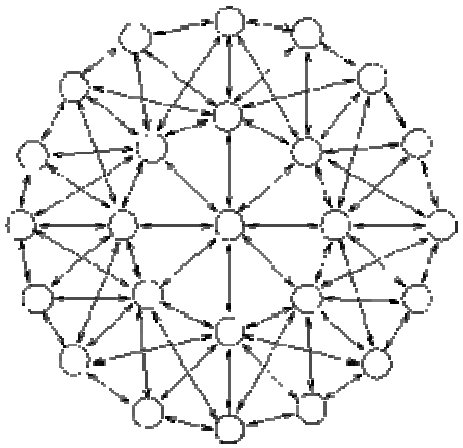

Figure 49. Packet Distribution During Flooding [24]

During the flooding process, each receiving station must process the packet in order to determine if it is relevant information. In the case where the station reads the same sequence number, it realizes that is has received a duplicate packet and discards it. That process is inefficient from the perspective of bandwidth and computer processing management. Figure 50, shown below, demonstrates the same process through the implementation of MPRs. The MPR flooding process greatly reduces the number of duplicate packages received and provides greater efficiency in bandwidth and computational processing management. Only the MPRs (nodes represented in black) retransmit the message. Consequently, the message is retransmitted four times versus the 24 retransmissions in the scenario above.

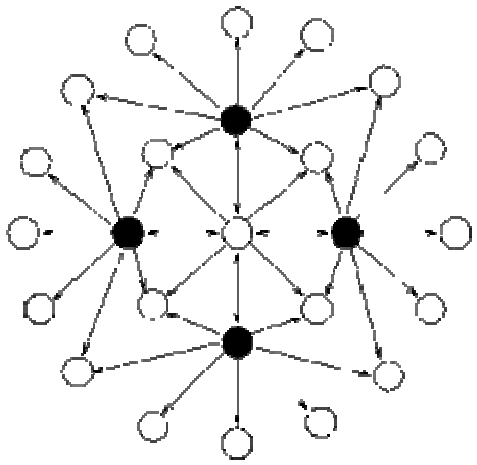

Figure 50. MPR Controlled Flooding [24]

MPRs are selected from among one-hop neighbors that have bi-directional linkages. The term "symmetric" is used in the Request For Comments (RFC) 3626 to describe these bi-directional linkages. Though the underlying link-layer actions function independently of the OLSR protocol, this policy prevents the selection of MPRs that do not provide for link-layer acknowledgement.

Three message types provide the core functioning of the OLSR protocol. The three message types are Hello-messages, Topology Control (TC)-messages, and Multiple Interface Declaration (MID)-messages. Hello-messages serve three independent tasks: link sensing, neighbor detection, and MPR selection signaling. TC-Messages are used to perform the task of topology declaration. This advertises the link states to the nodes on the network. MID-messages are used to perform the task of declaring the presence of multiple interfaces on a node. For example a laptop computer could have both a wireless interface as well as a wired interface, which would be advertised through MID-messages.

For this research, the OLSR protocol was tested on the D-DACT, which uses the PocketPC 2003 operating system, and on Panasonic Toughbook CF-48 and CF-73 laptops operating the Windows 2000 and Windows XP operating systems respectively. Fully operable implementations of OLSR are readily available on the Internet for

download and the protocol provides developers the ability to add desired functionality. The specific version used for testing in this thesis was modified by CenGen to support the C2CE application.

D. CENGEN OLSR MODIFICATIONS

As discussed previously in Section B of this chapter, CenGen is conducting ongoing research for the Office of Naval Research using the SecNet-11 PCMCIA wireless card. In order to mitigate the short transmission range of the card, they implemented OLSR mobile ad-hoc networking to provide delivery of information across links greater than one hop. As discussed in Section B of this chapter, this functionality is not possible with 802.11b products in ad-hoc mode.

CenGen selected a version of OLSR developed by NRL because the implementation was readily available and their desire was to leverage existing work rather than create a new application. CenGen had specific adaptations and functionality they wanted to add to the core OLSR service given the tools and environment of their research, specifically, the use of the SecNet-11 PCMCIA card, the D-DACT rugged handheld computer, and the Command and Control Compact Edition (C2CE) software.

The first task to be accomplished was to port OLSR functionality to a PocketPC operating system, as this was a requirement when using the D-DACT. The second task to be addressed was the layer two broadcast that C2CE software uses to transmit position location information (PLI) to other C2CE and C2PC clients in the network. C2CE and C2PC applications also use multi-casting in order to deliver the common operational picture to client machines, and CenGen had to add this capability to the OLSR protocol. Multi-casting allows for the efficient transmission of information from one to many nodes in the network. [26]

As discussed previously in Section C "Optimized Link State Routing," a MANET network can work as a stand-alone network independent of any other activity; however, this fails to realize the interconnectedness that can be provided through a point of presence (POP). The POP during experiments with CenGen and during this thesis research was generally provided by a laptop using a wireless interface to join the MANET cloud and a wired interface to participate on a second network. This computer

was commonly referred to as the OLSR bridge or gateway. Figure 51 below is a network diagram of the architecture employed at CenGen during testing in February 2005. It shows the OLSR bridge as a member of the SecNet-11 MANET cloud as well as a second wired network. The wired network shown in this diagram is housed inside the CONDOR vehicle, shown on the right side of the network diagram.

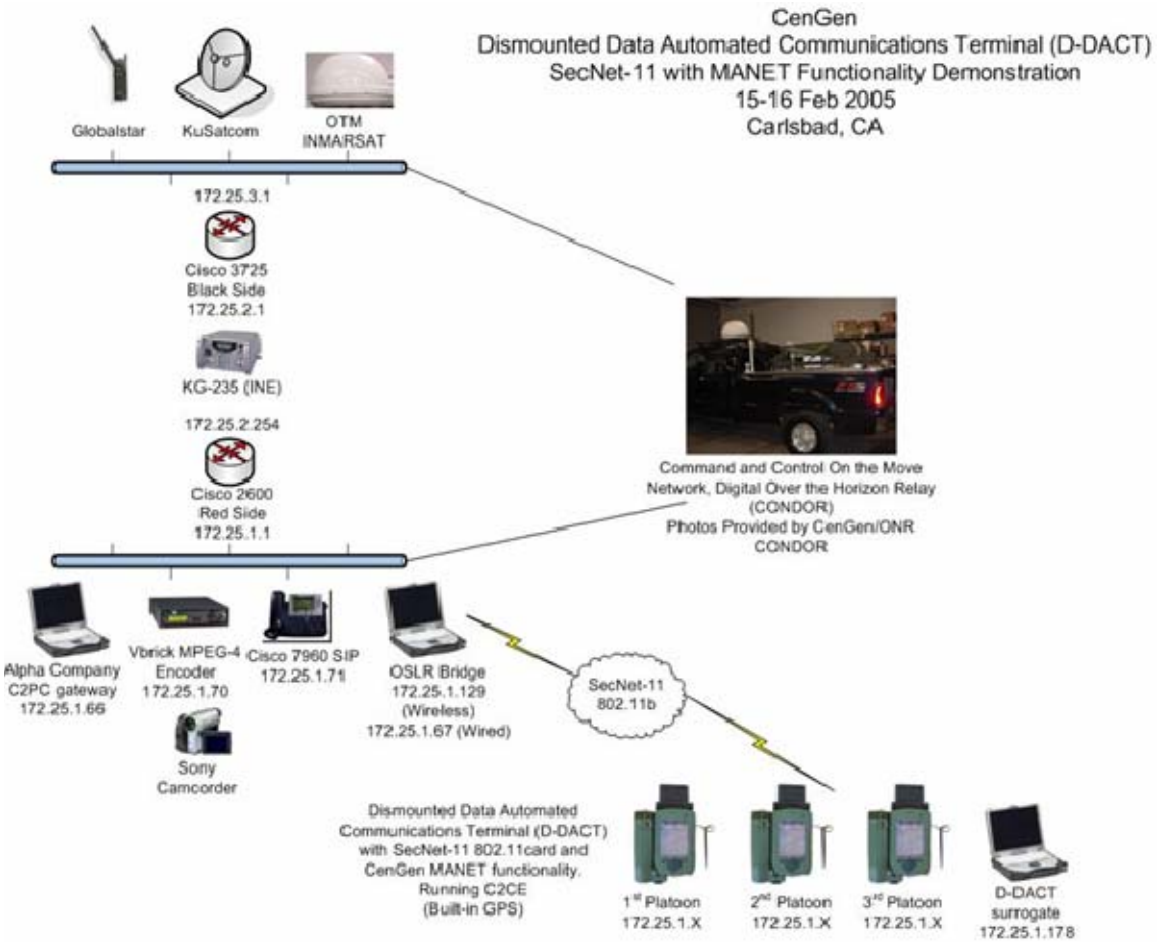

Figure 51. Network Diagram for MANET Demonstration at CenGen

One of the adaptations CenGen made was to enhance the gateway functionality in order to better support MANET to non-MANET operation. Lastly, they worked closely with Harris Corporation to update SecNet-11 drivers to allow the card to support the promiscuous mode for the PocketPC operating system. These new drivers met the multicast requirements.

The OLSR software that CenGen modified was tested on the D-DACT with the PocketPC 2003 operating system as well as on Panasonic Toughbook CF-48 and CF-73 laptops with Windows 2000 and XP operating systems. The Pocket PC version has a graphical user interface (GUI) that requires three clicks of a stylus to initiate; one click to open the program from the File Menu, a second to open the OLSR configuration screen, and a third to start the program. Figure 52 below shows the OLSR GUI.

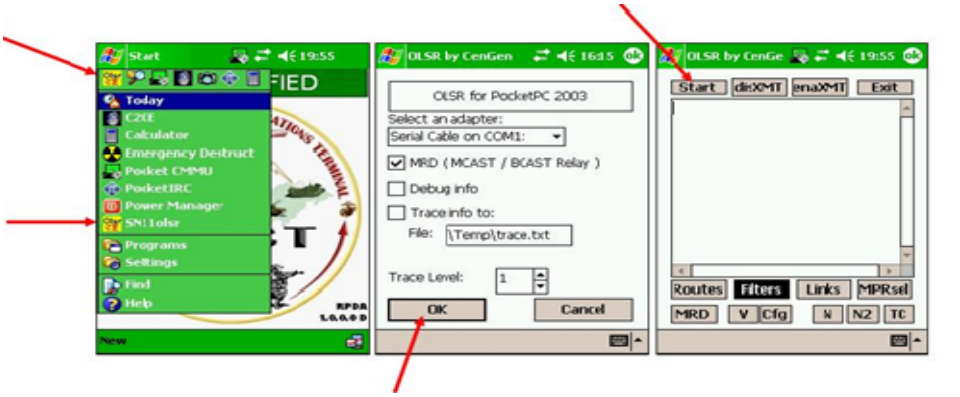

Figure 52. Starting CenGen's PocketPC OLSR Application

CenGen has yet to create a GUI to launch their OLSR application from Windows 2000 and XP operating systems. On these machines, OLSR is launched from the DOS command line. There is a help file the user can reference, and the software is easy to operate once the user has used it once or twice. Figure 53 below shows the DOS command line when launching the OLSR application.

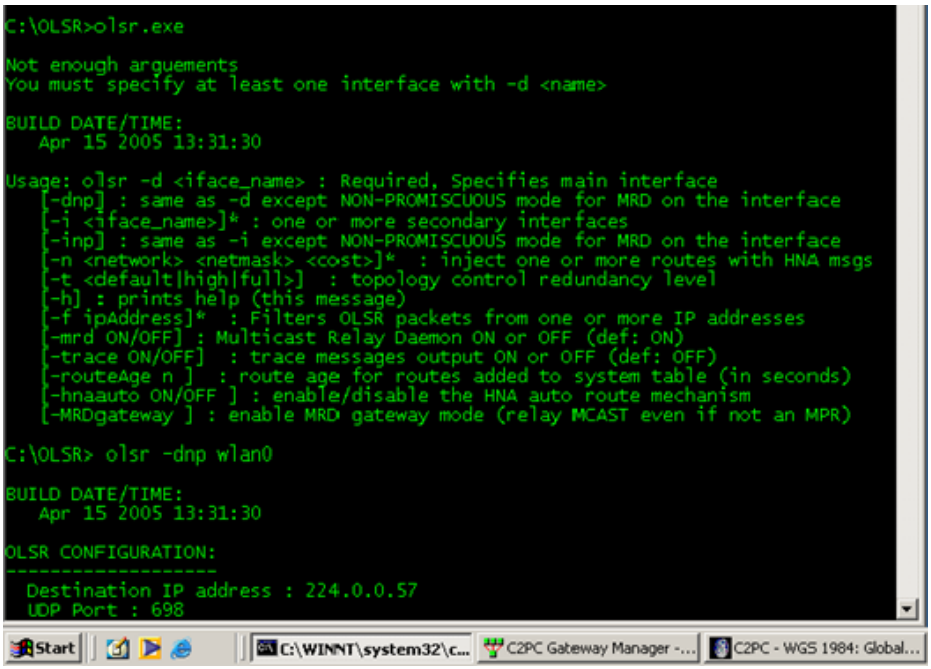

Figure 53. Launching CenGen's Windows 2000 and XP OLSR Application

The modifications CenGen made to the OLSR software worked well to support the C2CE application on the D-DACTs. In subsequent chapters, the performance of the devices using OLSR is discussed in greater detail. As mentioned earlier, one drawback is not having a GUI for the Windows 2000 or XP operating systems; if CenGen's modifications prove beneficial to other potential users, then the GUI could be created to enable easier access and use.

E. IEEE 802.16 PART 16: AIR INTERFACE FOR FIXED BROADBAND WIRELESS ACCESS SYSTEMS

The IEEE 802.16 standard was originally published in April 2002, after some amendments and improvements the standard is now known as IEEE Standard 802.16-2004. It is the IEEE standard for local and metropolitan area networks: Part 16: Air Interface for Fixed Broadband Wireless Access Systems. This standard was released in October 2004. The original standard focused on the frequency range between 10 to 66 GHz, the 2004 standard encompasses the 2-11 GHz range, which was the range on which this thesis focused. The research contained in this thesis is an extension of prior work done by Captains Guice and Munoz in their masters' thesis titled "IEEE 802.16

Commercial Off The Shelf (COTS) Technologies as a Compliment to Ship to Objective Maneuver (STOM) Communications." While Captains Guice and Munoz thesis looked solely at using this technology in STOM operations, this present research focused on employing 802.16 at the tactical level, not only in STOM, but in Distributed Operations as well. [27]

The IEEE 802.16 is commonly referred to as "WiMAX," which stands for Worldwide Interoperability for Microwave Access. WiMAX is now a certification mark for products that pass conformity and interoperability tests for the IEEE 802.16 standard. This is similar to the WiFi mark that you find on 802.11b equipment. IEEE 802.16 is working group number 16 of IEEE 802, specializing in point-to-multipoint broadband wireless access. Other terms commonly used that refer to 802.16 technology is HIPERMAN and WiBro. HIPERMAN is WiMAX'S equivalent in Europe and stands for High Performance Radio Metropolitan Area Network. WiBro is Korea's version, which differs slightly. Intel Corporation and LG Electronics, two major supporters of WiMAX, have agreed on trying to make all three interoperable. [28]

WiMAX is both faster and has longer range than WiFi. WiMAX does not necessarily conflict with WiFi, but is designed to interoperate with it by internetworking which would complement the network architecture. Most of the interest today is in the lower frequencies between 2 and 11 GHz. At these lower ranges, the signals can penetrate barriers and is better for NLOS communication links.

802.16 implements a multi-carrier transmission technique knows as orthogonal frequency division multiplexing (OFDM). OFDM has been around since the 1960's, but until recently, the high-speed chipsets necessary have been cost prohibitive. OFDM effectively squeezes multiple modulated carriers tightly together, reducing the required bandwidth, but keeping the modulated signals orthogonal so they do not interfere with one another. Figure 54 shows an example of this. OFDM essentially achieves high data rates by dividing a single communications channel into a larger number of closely spaced sub-carriers.

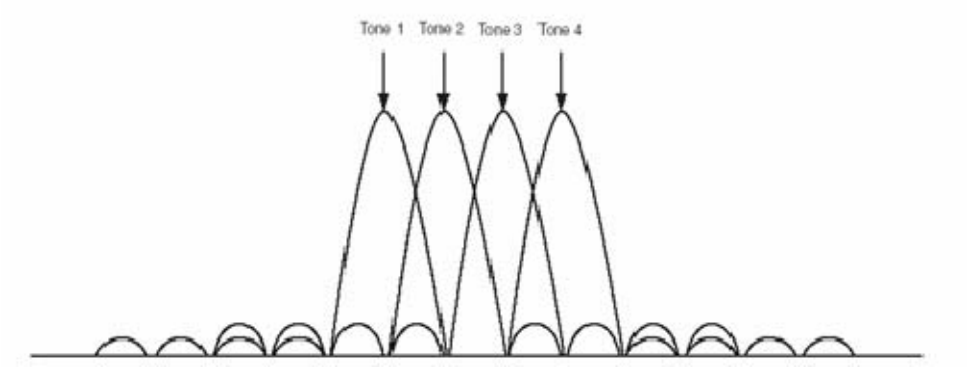

Figure 54. OFDM Illustration [29]

Each peak represents a sub-carrier, also known as a tone. Each tone individually has a relatively low data rate, but by transmitting data in parallel on all sub-carriers simultaneously, high data rates can be achieved. Other benefits of OFDM are

1. Handles large delay spreads more easily due to the independence of the carriers
2. The waveform can be easily modified to adjust to the delay spread of a channel
3. Allows efficient operation in both FDD and TDD mode, as very short or no pre-ambles are needed
4. Robust in adverse channel conditions and allows NLOS operation while maintaining a high level of spectral efficiency
5. Allows the use of contention timeslots, which increase MAC efficiency
6. Lower susceptibility to multi-path distortion.

As mentioned earlier one of the main reasons for testing the 802.16 equipment with the D-DACT's was to follow-up on earlier work and suggestions that Captains Guice and Munoz made while doing research on their thesis. One suggestion made was that a reliable solution for MANET was needed for operations like STOM. That was the main impetus for testing the D-DACT's mesh capability using the SecNet-11 cards with CenGen's software. In order to have the network extend out and give it the flexibility needed for being mobile, the importance of meshing is critical. The true mobility aspect

is not there yet for 802.16, but Redline has a product called the AN-50e Field Terminal (FT) that is portable and would be a quick way to set up a link for something like STOM or Distributed Operations. The AN-50eFT is discussed further in the next section.

The other suggestion was mentioned by another student at the Naval Postgraduate School concerned the security issues of the IEEE 802.16 standard and conducting field experiments with the equipment for viable applications to the military. Lieutenant Derrick Boom's thesis titled "Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks," looked at the MAC layer of the IEEE 802.16 standard to determine if it had similar vulnerabilities as the IEEE 802.11b standard. Although vulnerabilities are not covered in the scope of this thesis, it should be noted that the growing popularity and demand for these new products using the IEEE 802.16 standard should be taken into consideration. Understanding the security issues involved before implementing such networks is very important before relying on such communication links in real military operations. As a suggestion for future work by Lieutenant Boom, this thesis focused on conducting field testing in tactical environments to develop practical military applications for this type of technology. Assessing the vulnerabilities associated with this tactical WLAN was beyond the scope of this thesis.

F. REDLINE COMMUNICATIONS IEEE 802.16 BASED PRODUCTS

Redline Communications was the vendor chosen for the 802.16 equipment tested in these experiments. Redline Communications is based in Canada and designs and manufactures IEEE 802.16 standards-based broadband wireless access solutions. It should be noted that the equipment tested was pre-802.16-2004 and does not meet the WiMAX certification. This same equipment is currently being used in Iraq by the United States Marine Corps and in New Orleans to help the local agencies with communications while they recover from Hurricane Katrina. It was important to test the same equipment in order to determine its limitations along with benefits that may be derived for using it in future operations in the Marine Corps. The two main Redline products tested were the AN-50e and their manpack version of this same broadband wireless system along with various antennas. The AN-50e operates in the unlicensed 5.8 GHz band and supports

point-to-point (PTP) and point-to-multipoint (PMP) links. The AN-50e, shown in Figure 55, has the following features and characteristics:

1. Range of 50 mi in PTP mode with clear LOS and > 6 mi NLOS
2. Orthogonal Frequency Division Multiplexing (OFDM) technology for NLOS
3. Low end-to-end latency of 3 to 5 ms for time-sensitive applications like VoIP
4. Data rate of 72 Mbps in the air or 54 Mbps peak burst at MAC level
5. Dynamic time-division duplex (TDD) transmission
6. Eight modulation and coding schemes from Binary Phase Shift Keying (BPSK) to 64 Quadrature Amplitude Modulation (QAM)
7. Automatic repeat request (ARQ) algorithm with advanced forward error
8. correction
9. Support for Dynamic Frequency Selection (DFS) and Automatic Transmission
10. Power Control (ATPC)
11. Proprietary encryption scheme. [30]

Figure 55. Redline Communications' AN-50e

1. Setting Up and Configuring the AN-50e

Initial set up of the AN-50e requires a host computer to be connected to the terminal, as shown in Figure 56.

Figure 56. Laptop Connected to AN-50e at Ft. Ord

Once the connection is made, the default IP address or currently assigned IP address must be entered into the browser address bar in order to configure the terminal, as shown in Figure 57.

Figure 57. Default IP Address in Browser Address Bar

Once the correct IP address is entered, a login screen will appear in order to enter a user name and password, as shown in Figure 58.

Figure 58. Username and Password Screen

After successfully logging in, the user is taken to a general information screen shown in Figure 59 below. This gives the user information about what version software the equipment is running, whether or not a wireless link is established with a remote user, and if the system is in master mode. It is important to note, that only one system in the link can have the setting "yes" for master mode. The base station (BS) requires the master mode be selected. The remote end user, also known as, subscriber stations (SS) are marked "no" for this feature.

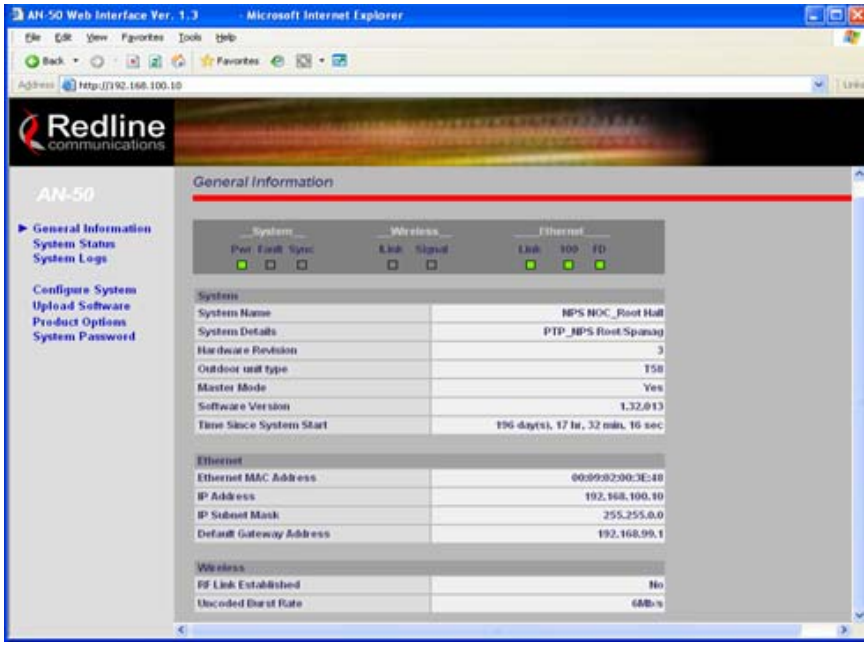

Figure 59. AN-50e General Information Screen

From the side menu, the user can choose the configure system option that will allow the user to change the settings on the terminal, as shown in Figure 60.

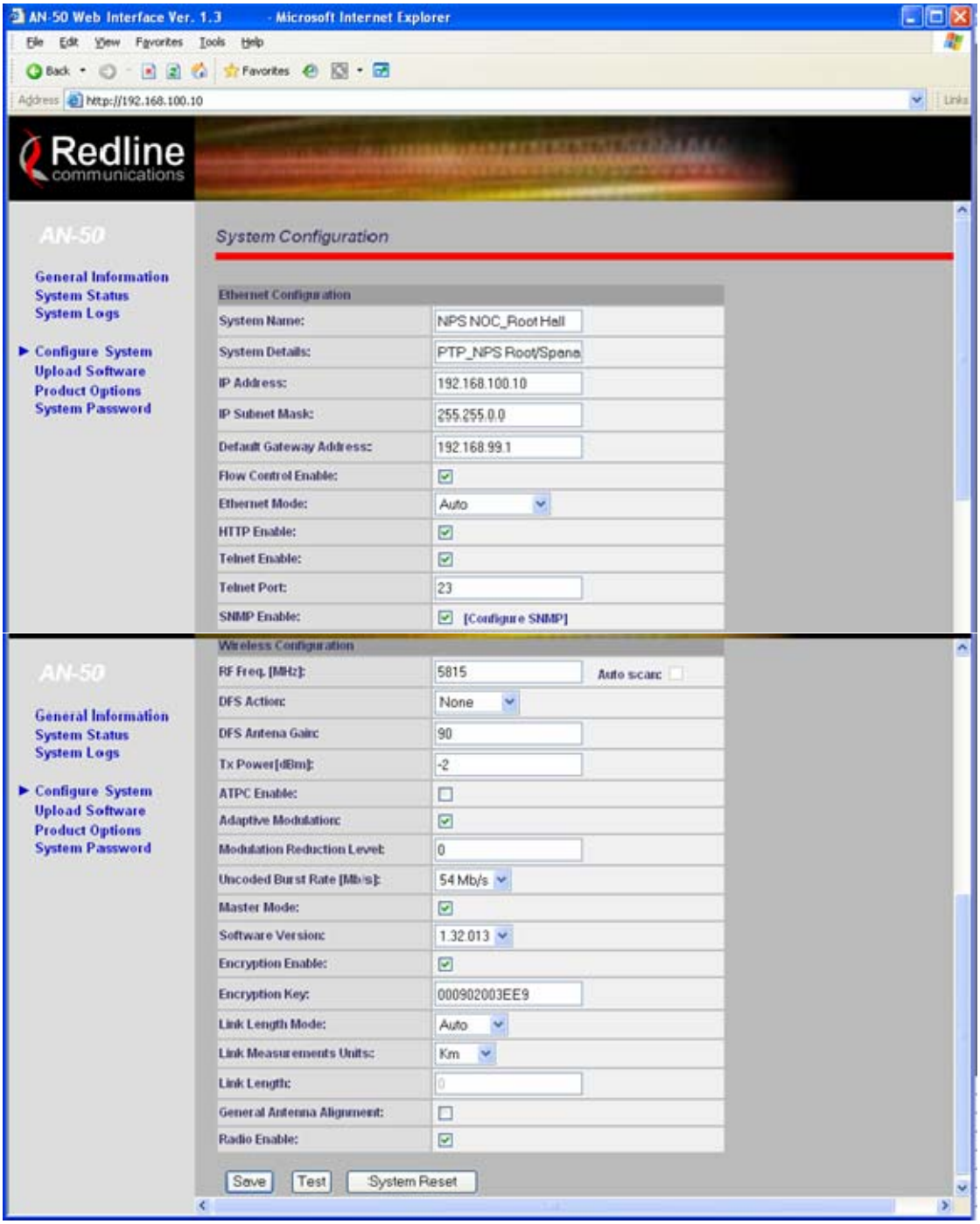

Figure 60. System Configuration Screen

Using the system configuration screen, the settings can be adjusted to fit the needs of the user depending on the IP addressing scheme, frequency, antennas employed, distance and how many SSs are connected to the base station. The settings in each field are divided by Ethernet configuration and wireless configuration. This is one of the first points to check when troubleshooting a link. If the data fields are incorrect or null values are entered, that could be enough to cause the communication link to not operate properly. The Ethernet configuration has features such as IP address, telnet enable, and SNMP enable. The wireless configuration has features to set the transmission power, the RF channel, and the antenna alignment. It also has a field to enable the built-in proprietary encryption. Checking the adaptive modulation check box ensures the system will automatically change the modulation scheme to the highest possible order based on the measured RF performance. Figure 61 below shows the maximum operational power per channel versus the modulation.

	64QAM ¾ (54 Mb/s)	64QAM ⅔ (48 Mb/s)	16QAM ¾ (36 Mb/s)	16QAM ½ (24 Mb/s)	QPSK ¾ (18 Mb/s)	QPSK ½ (12 Mb/s)	BPSK ¾ (9 Mb/s)	BPSK ½ (6 Mb/s)
Max Tx Power	14	15	19	20	20	20	20	20

Figure 61. Max. Operational Power Per Channel (dBm) vs. Modulation [31]

In Figure 62 below, the center frequencies of each permitted channel are shown. To avoid interference of two collocated links, it is imperative that each channel be separated by 20 MHz or more. So if channel 1 is at 5735 MHz then channel 2 should be at 5755 MHz. This is similar to having two 802.11b AP's near one another and assigning one AP channel 1 and the other channel 6.

Center Frequency	Center Frequency	Center Frequency
5735	5780	5825*
5740	5785	5830*
5745	5790	5835*
5750	5795	5840*
5755	5800	5845*
5760	5805	5850*
5765	5810	5855*
5770	5815	5860*
5775	5820*	5865*

*Pending approval.

Figure 62. North America: RF Channel Frequencies [31]

2. Antenna Set-Up and Alignment for the AN-50e

Several antenna types were employed during testing to include the two-foot flat panel and one-foot flat panel, shown in Figure 63 and 64 below.

Figure 63. Two-Foot Flat Panel Antenna

Figure 64. One-Foot Flat Panel Antenna

After mounting the antenna to a pole using the bracket as shown in these figures, alignment is the next crucial step. The antenna must be aligned in both the azimuth and elevation planes. In the system configuration, there is a check box for general antenna alignment. If this is checked, it will enable a chirping sound that helps the user align and tune the antennas to the strongest signal available. The faster the repetitions of the chirping sound, the strongest signal or best alignment available has been achieved. The red arrow on the right in Figure 63 is pointing to an alignment bolt. This is used to help make elevation adjustments. The yellow arrow on the left is pointing to the bolts that are used to adjust azimuth. Once the user is satisfied that the antennas are aligned, the user can return to the system configuration and uncheck the box to turn off the chirping sound. Table 7 below lists the specifications of antennas used.

Antenna	Weight	Size	Beam Width	Gain (dBi)
One-Foot Flat Panel	1.5 kg	30x30 cm	9°	23 dBi
Two-Foot Flat Panel	5.0 kg	60x60 cm	4.50°	28 dBi
Sector	N/A	65x21.6x19 cm	90° azimuth 8° elevation	14 dBi
Omni-directional	.68 kg	74.7x5.842 cm	6° vertical 360° horizontal	12 dBi
Omni-directional	0.4 kg	30x4 cm	6° vertical 360° horizontal	9 dBi

Table 7. Antenna Specifications [30]

3. AN-50e Field Terminal (FT) "Manpack"

The AN-50eFT manpack concept, shown in Figure 65, is Redlines' portable version of the AN-50e, which has the same characteristics and features, with a few minor exceptions. The manpack has an external slot for an omni-directional antenna to be affixed to it for the portability aspect and has been modified to operate from two Lithium external batteries. This allows the operator to power the manpack with disposable DC power as opposed to fixed AC power. The T-58 transceiver is mounted on top of the radio next to the batteries.

Figure 65. AN-50eFT Manpack [32]

The manpack was designed to be portable, but not mobile. It runs on two military BA-5590 12 VDC tactical batteries and will support the one-foot and two-foot flat panel antennas as well as the omni-directional. Current research is being conducted at NPS on the manpack with regards to ship-to-shore by Lt Chris Marvin in his Master's Thesis titled "802.16 OFDM Rapidly Deployed Network for Near Real Time Collaboration of Expert Services in Maritime Security Operations." The actual manpack being tested is shown in Figure 66 below.

Figure 66. AN-50eFT Manpack Radio

Lt Marvin used the AN-50eFT manpack radio in order to provide a wide area network (WAN) for the transmission of spectral graphs taken by the GN-5, which is a small mechanically-cooled Germanium Gamma-ray spectrometer. The wireless link was also used to transmit biometric data specifically, fingerprints, to a processing center for aiding in the identification of potential terrorists.

The experiments performed by Lt Marvin took place aboard the United States Coast Guard Cutter Hawksbill. Aboard the Hawksbill, the boarding team used the GN-5 to scan the ship for anomalous sources of radiation. When a source was detected, the GN-5 used a resident database to give the operator a preliminary analysis. The AN-50eFT was used to deliver the information to an ashore facility where there was an Internet POP. From the POP, the information was delivered to scientists at the Lawrence Livermore National Laboratory for further investigation.

Using this process, the boarding team was able to detect a radiation source, which the GN-5 identified as Thorium. This information was relayed to the POP via the Redline 802.16 wireless link at a distance of 2,000 meters to the shore facility. The throughput available was 925 kbps. Through further analysis the team at LLNL also detected the presence of Californium. Figure 67 below shows the GN-5 radiation Gamma-ray spectrometer.

Figure 67. GN-5 Portable, Mechanically-Cooled Germanium Gamma-Ray Spectrometer

The second experiment used the digital fingerprint solution by Cross Match Technologies, which captures fingerprints for analysis against stored fingerprints in a

database. The wireless 802.16 link was used again to deliver the fingerprint data to the ashore POP where it was delivered for processing to the Biometric Fusion Center in West Virginia. Within twenty minutes, a simulated suspect aboard the Hawksbill had his fingerprints taken and processed in BFC and was identified as a suspected terrorist and apprehended. Figure 68 shown below is the Cross Match fingerprint system.

Figure 68. Portable Fingerprint Solution

Those interested in a more in-depth review of the test scenario, objectives and measures of performance related to this mobile 802.16 wireless link should read Lt Marvin's analysis.

4. Link Budget Calculation

An understanding of the output power for 802.16 wireless devices as well as the gain of the antenna employed is crucial in estimating the range these systems can support. Redline Communications receivers must receive sufficient signal strength from distant stations in order to process the information being sent. A conservative estimate is that the receiver should have received signal strength of at least -80 dBm. Redline Communications claims their equipment can support ranges of approximately up to 50 miles. This approximate range is calculated using the FSPL equation.

$\text{Path Loss}_{(dB)} = 20*\text{Log}_{10}[(4*\pi*D)/\lambda]$

D= distance (in like units as λ)

λ= wavelength calculated as c/f (C=speed of light f=frequency)

Using the FSPL equation, for a distance of 50 miles (80.5km) and a frequency of 5765 MHz returns a path loss of 145.77 dB. This means that over a span of 50 miles a wireless device transmitting at 5765 MHz will lose 145.77 dB due to FSPL. To complete this example, use the attributes provided in Table 8 below.

Transmit Power	+14 dBm
Transmitter Antenna Gain	+34.8 dBi
Transmitter Connector Loss	-9 dBi
Path Loss	-145.77 dBm
Receiver Antenna Gain	+34.8 dBi
Receiver Connector Loss	-9 dBi
	-80.77 dBm
Required Signal Strength	-80 dBm

Table 8. Redline Communications Range Example

This example demonstrates how this type of link could be supported. The AN-50e provides 14 dBm of transmit power when 64 QAM modulation is selected. The 34.8 dBi of gain is possible when employing a parabolic dish antenna that is 120 cm in diameter and weighs 60 lbs. The connector loss of 9 dBi is typical when the AN-50 is employed with 225 feet of Intermediary Frequency (IF) cable (RG-6U IF cable). This deployment does not take into consideration the height of the antenna in order to ensure the fresnel zone has a clear line of sight.

5. Current Deployments of Redline Communications Equipment

This equipment has been deployed around the world by a host of agencies trying to leverage the wireless capabilities in order to improve their communications. One example that proves the viability of this technology to meet specific requirements is the tactical employment of Redline equipment in Iraq supporting United States Marines. Also, the Marine Logistics Forces from the II Marine Expeditionary Force (MEF) required the ability to distribute wideband connectivity across the battlespace to tactical commanders. That requirement was supported by 2nd Force Service Support Group (FSSG) purchased four Very Small Aperture Terminals (VSATs) from the Army Program Executive Office Enterprise Information Systems (PEOEIS) office. This Ku-

band satellite would provide “NIPRNET and SIPRNET connectivity” in the battlespace through access to Defense Information Systems Network (DISN). [27]

The VSAT connectivity was to be distributed to several Forward Operating Bases (FOBs) and small military camps. The distribution equipment selected was Redline Communications pre-802.16 products. The Marine Corps employed Air Fortress software encryption devices in order to comply with directives requiring unclassified wireless links to have FIPS 140-2 equivalent protection. To provide SIPRNET enclaving KG-175 Taclane solutions were employed in order to create a secure tunnel. These inline encryption devices (INEs) are deployed throughout the MAGTF to deliver SIPRNET connectivity. Figure 69 below demonstrates a one-foot flat panel deployed at Camp Fallujah. This is one of 15 links deployed to provide both voice and data connectivity.

Figure 69. Redline Communications Deployed at Camp Fallujah, Iraq

Initial reports from communications personnel from Marine Corps Tactical Systems Support Activity (MCTSSA) indicate that the equipment is performing

extremely well. One wireless link mentioned specifically, spanned 16 miles between Camp Fallujah and Al Taqqaddum. This link was providing 9 Mbps of throughput. The deployment leveraged the AN-50e system with the software option supporting QPSK modulation with a maximum of 18 Mbps throughput. The system also employed the one-foot flat panel antennas. Discussions were underway to upgrade the systems to 64 QAM and to use the two-foot flat panels in order to support longer distances and higher throughput.

G. TACTICAL ANTENNA MASTS

In order to support communications in a tactical environment, military forces employ tactical antenna masts to elevate the radiating elements of their communications devices. The Marine Corps uses an OE-254 antenna mast with very high frequency (VHF) radio frequency hopping assets. The OE-254 raises the radiating element to a height of 42 feet. Raising the radiating element to this height greatly increases the range of communications, particularly for long-range communication links.

For this thesis, two tactical antenna masts were purchased in order to raise the antenna for IEEE 802.16 communication devices. Figure 70 below shows a 12 dBi omni-directional antenna on the tactical antenna mast. It was crucial to raise this antenna when it was connected to a Redline Communications 802.16 AN-50e radio with BS software. This base station was providing a point-to-multi-point wide area network (WAN) to three SSs. This deployment is discussed in further detail in Chapter V "Laboratory and Field Experimentation."

Figure 70. Tactical Antenna Servicing the Redline Communications Base Station

H. IXCHARIOT NETWORK ANALYSIS TOOL

IxChariot version 6.0 by IXIA was the software tool used to measure the system performance under various conditions throughout each experiment. IxChariot was created by Ixia, a publicly held company specializing in network performance testing tools. It is a very expensive COTS tool when compared to the free software available. But, it is well worth it and highly recommended. IxChariot was chosen mainly for its ease of use and reputation as being one of the best software tools available for monitoring and testing network throughput. One machine was loaded with the IxChariot console as shown in Figure 71.

Figure 71. IxChariot Console

The other devices connected to the network were loaded with IxChariot Performance Endpoints. It was necessary to load each device with this in order for the console to measure each independent node. Once the software was loaded, each laptop firewall had to be disabled in order for the tests to be run successfully.

Various options and tests can be performed using this tool. IxChariot can test up to 10,000 connections (endpoint pairs), which represent hundreds of thousands of end-users. The tool can also test different protocols and technologies, such as, TCP, UDP, RTP, IPv4 and 6, VoIP, and IP multicast. The performance endpoint is compatible with all Windows O/S including CE, Linux, and FreeBSD. [33] One of the main features that was very beneficial was that IxChariot has over 140 pre-programmed scripts from which to choose that are capable of emulating all of the common protocols and services. The pre-programmed scripts can be modified to suit the users needs as well. The experiments conducted for this thesis used the benchmark scripts. There are six different benchmark scripts to select from. The benchmark script used was the "Filesndl.scr" from the file transfer scripts. Filesndl.scr, stands for "File Send, Long Connection," which emulates requesting a file and receiving, and sending a file and receiving an acknowledgement. This particular script was used because it was determined that it would represent the type

of data that a tactical user would actually send during an operation. The file size used was 1 MB, which was determined to be the greater than the typical file size a tactical user would send and receive. [34]

I. MULTI-GENERATOR (MGEN) AND NETPROBE

Multi-generator (MGEN) is open-source software designed by the Naval Research Laboratory (NRL) that provides the ability to perform network performance tests and measurements using user datagram protocol (UDP) Internet Protocol (IP) traffic. The MGEN toolset generates real-time traffic patterns that allow the network administrator or user to load the network in a variety of ways. The generated traffic can be received, stored, and logged for future analysis. [28]

NRL currently provides two versions of MGEN on its website for download, versions 3.x and 4.x. These versions are not interoperable. Version 3.x comes with a simple graphical user interface (GUI) whereas version 4.x must be launched from the command line. The NRL site also provides an online user's manual to aid the user in downloading, installing, and operating the application.

This is a powerful application that is readily available and free; however, it is not for the command-line novice. This program requires an investment in time in order to master. The outputs from this program are in raw form and require another application in order to process and to display in an easily understood format. Steve Durbano developed several MATLAB scripts to take the raw data files, process them, and produce plot graphs of the results for visual analysis. CenGen uses MGEN to test the performance of the network when using both uni-cast and multi-cast traffic and uses the data to analyze network performance with respect to packet loss, delay, and packet sequencing.

NetProbe is a second freeware network monitor and protocol analyzer that runs on the Microsoft family of operating systems, Windows NT/2000/XP as well as Linux, FreeBSD, Solaris, and Mac OS X. [29] CenGen uses the tool to measure accurately the latency and jitter between to end points on a network. Like MGEN, described above, NetProbe is launched and operated from the command line. This tool requires a

significant level of proficiency from the user. Once again, as with MGEN, Steven Durbano developed MATLAB scripts that take the raw NetProbe data and produce plot graphs.

These tools were described briefly in order to mention network monitoring and analysis tools that are free and can provide powerful analysis of network performance. Several graphs produced by Steven Durbano of data captured during field experimentation at Camp Roberts, CA, during Tactical Network Topography (TNT) are presented in Chapter V of this thesis.

J. SUMMARY

This overview began with Harris' SecNet-11 product line and the Optimized Link State Routing Protocol (OLSR), which was used to overcome the short transmission distance of IEEE 802.11b PC cards. The overview then proceeded to explain adaptations made by CenGen for these technologies used in the D-DACT and C2CE applications. From here, the overview addressed the IEEE 802.16 products that provided the WAN connectivity and concluded with information on several network analysis tools used to record throughput metrics.

V. LABORATORY AND FIELD EXPERIMENTATION

The experimentation conducted for this thesis spans eleven months. Each experiment added to the understanding of the strengths and weaknesses of these technologies, and as such this chapter progresses chronologically through the experiments performed. This chapter also represents major testing evolutions designed to answer specific questions and to meet the predetermined objectives for this thesis. This chapter describes each test scenario and corresponding objectives, presents the measure of effectiveness, and lastly provides results of each test and the lessons learned.

A. COALITION OPERATING AREA SURVEILLANCE AND TARGETING SYSTEM (COASTS) EXPERIMENTS

1. Background

The Coalition Operating Area and Surveillance Targeting System program is an ongoing research program at the Naval Postgraduate School, working to leverage new wireless technologies that can support the Royal Thai Military's efforts to improve security and to combat the global war on terrorism (GWOT). The COASTS program is sponsored by U.S. Pacific Command (USPACOM) and is modeled after the Tactical Network Topology (TNT) experiments, which are tasked with integrating emerging wireless local area network (WLAN) technologies with surveillance and targeting hardware/software systems to augment Special Operations Forces missions. [30]

The COASTS program was designed to leverage and integrate the technological expertise of NPS's education and research resources with the science and technology (and potential operational requirements) of the Royal Thai Supreme Command (RTSC) using WLAN technologies to fuse and to display information from air and ground sensors to a real-time, tactical, coalition enabled command and control center. [30] COASTS provided an opportunity to operate Redline Communications IEEE 802.16 - based equipment in an environment far different from that of either Monterey or Paso Robles, CA, where TNT field experiments are conducted.

2. Network Architecture

The network that was designed for COASTS was intended to support real-time video and situational awareness tools from IEEE 802.11b devices that would be backhauled by Redline Communications equipment to a point of presence (POP) for transmission via one T-1 and one E-1 connection. The real-time video and situational awareness applications would ultimately be displayed at the RTSC Headquarters who would be able to control the IP based cameras as well. Figure 72 below shows the network diagram created to support the described concept of operations.

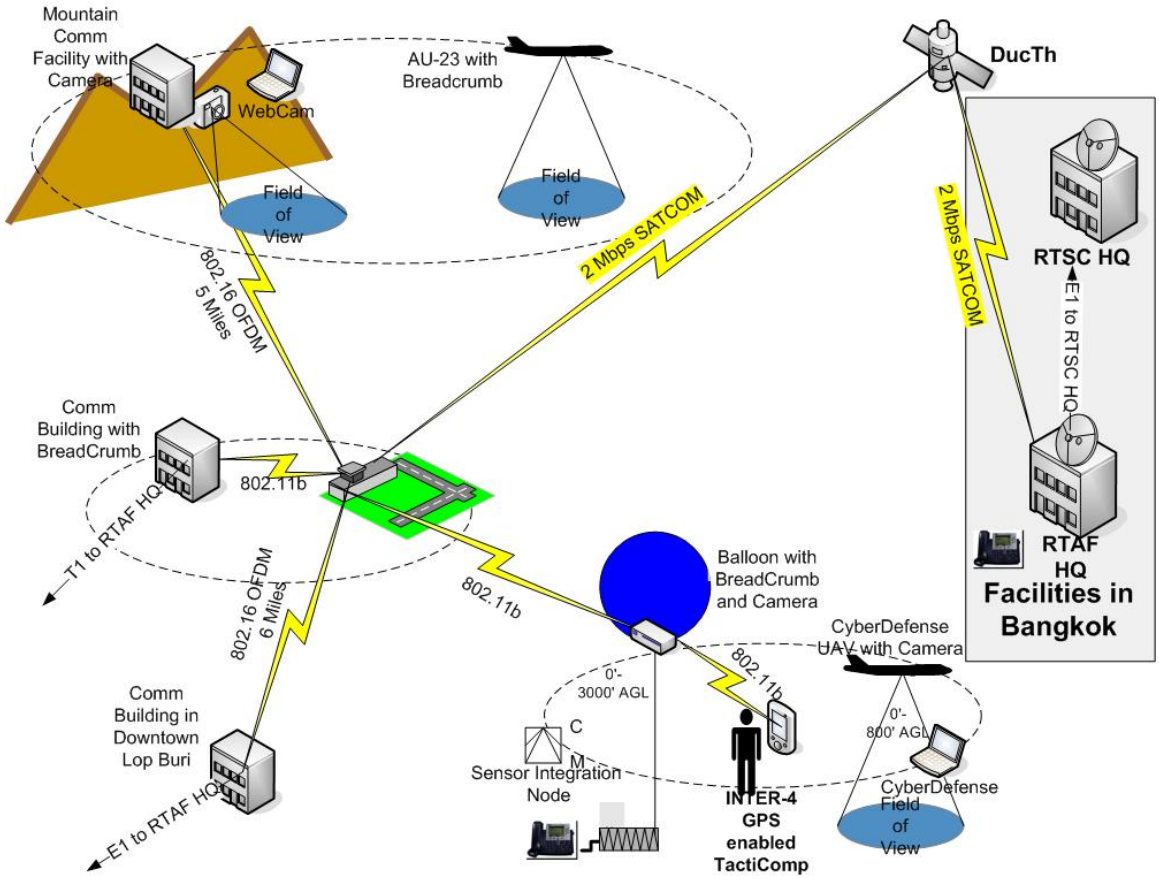

Figure 72. COASTS Network Diagram

Figure 72 represents the COASTS network diagram. The crucial elements are the two Sony cameras located at the Mountain Communications Facility (MCF) and on the tethered balloon, and the Tacticomp operating within an 802.11b ad-hoc network. The satellite service was later provided by an external agency through an arrangement with

the Royal Thai Air Force (RTAF). Two 802.16 point-to-point links were required in order to connect the Sony camera at the MCF to the Tactical Operations Center (TOC) in the Airfield Tower. All the tactical information at the TOC was delivered to the Range Two communications building where there was a T-1 connection to RTAF headquarters in Bangkok.

The second 802.16 link backhauled all traffic from the TOC to the communications building in downtown Lop Buri where there was an E-1 connection to RTAF headquarters in Bangkok.

3. Pre-Deployment Exercise (February 2005)

Prior to deploying the equipment to Thailand several large experiments were conducted in Fort Ord, CA, to test the operational capabilities of the equipment and the proposed network architecture. The test scenario used Nemesis, which is a 24-foot recreational vehicle that has been modified to contain internal generator power, networking equipment, and computer assets in order to serve as a mobile operations center, to replicate the TOC at the Range Two Airfield Tower. Nemesis would house a Cisco router and 802.16 connections in order to recreate the network architecture described above in Figure 72.

Table 9 below describes the tasks to be accomplished during the exercise, as well as a status of the task and a remarks column that provides more detail on the specific task.

TASK	STATUS	REMARKS
Establish a point-to-point link using 1-foot flat panel antennas in order to simulate the 802.16 link between Mountain Communications Facility (MCF) and the Tactical Operations Center (TOC).	Accomplished	54 Mbps uncoded burst rate
Establish a point-to-point link using 2-foot flat panel antennas in order to simulate the 802.16 link between the Downtown Lop Buri Communications building and the TOC.	Accomplished	54 Mbps uncoded burst rate
Using a layer 2 switch, attach a host computer to the Redline AN-50e simulating the MCF and downtown Lop Buri building deployment. Use these computers to test the wireless link by performing a ping from the command line.	Accomplished	Echo Response < 5 milli-seconds (ms)
Using a layer 2 switch, attach a host computer to the Redline AN-50e simulating the MCF and downtown Lop Buri building deployment. Use these computers to access the TOC file server, other nodes on the network, and the Internet. This simulates distant stations accessing resources at the TOC, as well as accessing the POP for Internet connectivity.	Accomplished	TOC server, and Internet accessed.
Establish an 802.11b WLAN using WE Breadcrumb (SSID Mountain) that hangs off the simulated MCF 802.16 link. One computer will associate to WE Breadcrumb. Then accomplish tasks 3 and 4.	Accomplished	Echo Response < 5 ms, TOC server and Internet accessed.
Establish an 802.11b WLAN using WE Breadcrumb (SSID Lop Buri) that hangs off the simulated Lop Buri building 802.16 link. One computer will associate to WE Breadcrumb. Then accomplish tasks 3 and 4.	Accomplished	Echo Response < 5 ms, TOC server and Internet accessed.
Use the WLAN and 802.16 back haul to transmit streaming video across the network using laptop (i.e. Panasonic CF-48) and Tacticomp.	Not Accomplished	Not enough time allotted during experiment.
Use the WLAN and 802.16 back haul to test Voice Over IP functionality with headset on Tacticomp.	Not Accomplished	Not enough time allotted during experiment.
Use Panasonic CF-48 laptops and Tacticomp associated on the WLAN with 802.16 back haul to control Sony camera across the network.	Partially accomplished	Task executed from laptop. Tacticomp did not have required drivers installed.
Use Panasonic CF-48 laptops and Tacticomp associated on the WLAN with 802.16 back haul to operate Situational Awareness software.	Not Accomplished	Situational Awareness application still under development at this time.
Conduct network operations	Accomplished	
Measure and evaluate the ease of installing, operating, and maintaining an 802.16 wireless network, and the completeness and accuracy of the shared common operational picture provided to the tactical user.	Accomplished	Several lessons were learned and described in detail in AAR.
Explore and capture techniques, tactics and procedures, which can be leveraged in further testing.	Accomplished	Several lessons were learned and described in detail in AAR.

Table 9. Task and Measures of Effectiveness for COASTS Pre-Deployment Exercise

Most tasks were accomplished successfully, and those that were not could have been accomplished if more time had been allotted for the exercise, or if the Situational Awareness application had been delivered for integration during testing. Based on the test results, there was a sense that the architecture, as designed, would support the requirements once the COAST team deployed to Thailand.

Several key observations were made during this exercise. First was the importance of an effective sight survey. The operation of equipment in the 5 GHz spectrum and with directional antennas requires line of sight. During initial set-up a chain-link fence partially obstructed one antenna and a metal shed building was 20 meters in front of the second antenna. These obstructions prevented the establishment of the 802.16 link, requiring the antennas to be moved to more advantageous terrain.

4. COASTS Deployment to Thailand (March 2005)

Twelve members of the COASTS team deployed to Thailand on the 14th of March 2005. The task was to establish IEEE 802.11b and 802.16 wireless networks to enhance the situational awareness of the RTSC headquarters as described in the background section. The preparations made during exercises at Fort Ord, CA, and at the Naval Postgraduate School proved extremely beneficial as they allowed the gear to operate as intended once deployed in the RTAF Range 2 facility.

The link from the airfield tower to the MCF proved challenging because a single team member was inserted via helicopter to install the equipment. His efforts to mount the one-foot flat panel antenna on a radio tower, communicate on a cell phone with poor cell coverage, and align the antenna to the antenna five miles away at the airfield tower was very challenging, shown in Figure 73 below. The equipment was successfully installed and a link of 18 Mbps was established at a distance of five miles. When a second team member deployed to the MCF, the link was improved to 36 Mbps. With proper equipment and additional time, this link could have been improved to a 54 Mbps uncoded burst rate.

Figure 73. One-Foot Flat Panel Antenna at the Range Two Flight Line

The link from the airfield tower to downtown Lop Buri required a considerable investment in personnel, time, and resources in order to install it. The two-foot flat panel antenna was installed on a 70-meter tower in downtown Lop Buri. Due to a treeline that was adjacent to the tower, COASTS personnel had to climb to a height of approximately 50 meters to ensure line of sight. Climbing to that height while using an improvised pulley system to raise the antenna and mount it to the structure required considerable effort. Compounding the problem was the lack of proper tower climbing equipment and trained personnel. The importance of a proper site survey was once again the largest lesson learned during this deployment as well as ensuring the installer possessed the necessary skills to install the equipment successfully.

Little was known about the installation site until the team arrived at Lop Buri and the time needed to install the equipment limited other aspects of the exercise. Despite the setback due to the installation time required at the Lop Buri tower, the 802.16 link back to the airfield tower was successfully established at a distance of six miles and delivered 54 Mbps uncoded burst rate.

Both 802.16 point-to-point links worked as designed and proved to be solid performers throughout the exercise, once they were installed. The links were powered off daily at the conclusion of the workday and restarted the next morning. Each time, the

gear initiated as expected and delivered the same throughput as the day they were installed. The links successfully bridged traffic from the MCF to the TOC and from there all exercise traffic was delivered to the Range 2 POP and the downtown Lop Buri POP for delivery to RTSC headquarters in Bangkok via E-1 and T-1 lines. Personnel at RTSC headquarters were able to control the Sony camera at the MCF as well as the camera mounted on the balloon node.

This deployment proved to be a great learning experience as well as a benchmark for installing Redline Communications equipment, in the humid environment of Southeast Asia versus the conditions in the California Central Coast. The weather did not affect the performance at that time.

B. D-DACT TESTING AT CONSULTING AND ENGINEERING NEXT GENERATION NETWORKS (CENGEN) AND MARINE CORPS TACTICAL SYSTEMS SUPPORT ACTIVITY (MCTSSA)

1. Background

Building upon the experiments conducted with COASTS, the authors sought a method to incorporate the D-DACT and SecNet-11 into future experiments in order to conduct research on assets the Marine Corps was currently employing. Personnel at the Marine Corps' Tactical Systems Support Agency (MCTSSA) were conducting experiments of their own in order to evaluate the performance of the D-DACT, and Command and Control Compact Edition (C2CE) software in their testing facility at Camp Pendleton, CA. The test employed assets described in Chapter III "Overview of the Tactical Internet," specifically the SINCGARS, and EPLRS radios, D-DACTs, M-DACTs, IOWs and IOSs. The scenario is discussed in greater detail in the next section.

Personnel from CenGen were also conducting testing with the D-DACT but were using the SecNet-11 PCMCIA card in order to provide the communications link instead of using the AN/PRC-119 SINCGARS radio. This testing took place outside the gates of Camp Pendleton in Carlsbad, CA.

Both organizations allowed us to observe testing and offered a great deal of continuing support during the entire eleven months of thesis research. Their assistance in this process was indispensable.

2. D-DACT Testing over Tactical Networks (November 2004)

Captain Jordan Reece is the DACT technical support officer at MCTSSA and was directly responsible for the testing and evaluation of the system as currently deployed to the Marine Corps. His team of engineers, as well as contractor support teams from Titan, Raytheon Fort Wayne (RFW), Northrop Grumman Mission Systems (NGMS) and Ocean Systems Engineering Company (OSEC) were present in November 2004 in order to conduct exhaustive testing of the entire system.

This specific test called for nine D-DACTs each connected to an AN/PRC-119 SINCGARS radio, three M-DACTs each connected with dual interfaces to an AN/PRC-119 SINCGARS and EPLRS radio. Platoon D-DACTs were configured to send PLI and track data to their respective company via SINGARS, and each company M-DACT was configured to transmit traffic to the battalion C2PC gateway machine via the EPLRS radio. Figure 74 below describes the network design for the test.

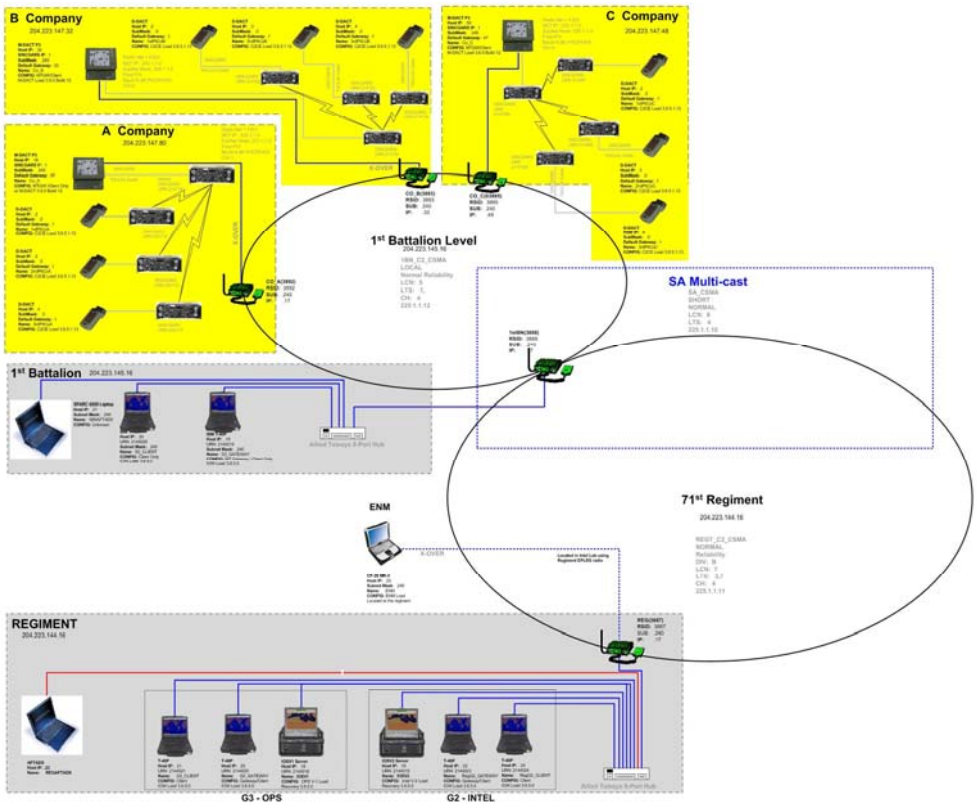

Figure 74. D-DACT Network Evaluation

The objectives of the test were to evaluate the D-DACT performance in its Federation of Systems (FEDOS) / System of Systems Test (SoST) 04 form using two separate software builds. The first test was required in order to evaluate updates that had been completed to a previous build. The subsequent test evaluated the latest software release.

The conclusion of testing was that errors encountered during the previous round of testing had been greatly reduced; however, issues regarding all hosts on the network displaying the same common operational picture remained.

The observation of this testing proved critical for several reasons. First, observing the test familiarized us with the equipment and its employment within the Marine Corps. Secondly, we could ask specific questions to subject matter experts within their specific domains. For example, questions regarding the Taclink 3000 card could be presented to RFW personnel, and questions pertaining to C2CE could be addressed by NGMS personnel. Lastly, this experience established working relationships that proved vital throughout the course of the research.

3. D-DACT OLSR Demonstration (February 2005)

This demonstration at CenGen's Carlsbad, CA, office was one of the most relevant exercises. It demonstrated what work had been accomplished with the D-DACT, OLSR protocol, and SecNet-11 PCMCIA cards. The working relationship established with Steven Durbano at CenGen proved essential to our research. The laboratory testing observed at the CenGen office became a model worthy of emulation.

The operational scenario observed at the CenGen office was an advanced implementation of D-DACT, and M-DACT nodes centered on a Marine Corps rifle company. Three D-DACTs were used to represent 1st, 2nd and 3rd platoons of a rifle company. A Panasonic Toughbook CF-72 served as an OLSR bridge, using dual interfaces, one to participate on the secure wireless local area network (SWLAN) and the second to participate on the wired portion of the network. The D-DACTs were configured to deliver PLI and track data to the Alpha Company C2PC gateway machine, which simulated the company commander's M-DACT. Figure 75 below represents the architecture CenGen employed in order to test the C2CE and C2PC functionality.

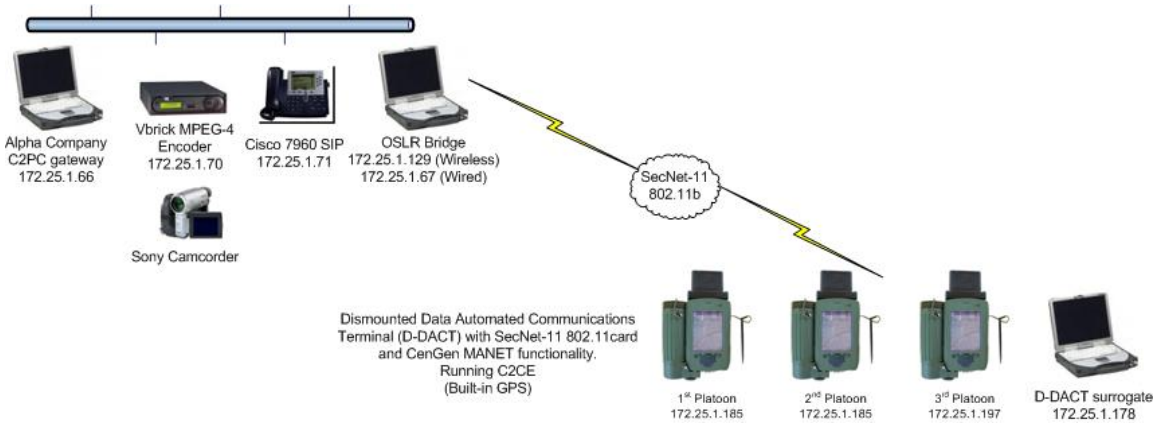

Figure 75. CenGen SecNet-11 SWLAN Network

As shown in Figure 75 above, CenGen leveraged an MPEG-4 encoder to deliver real-time data over the network and CISCO IP telephony in order to provide Voice-over-IP (VoIP) functionality. That functionality was beyond the scope of this thesis, but provides an area for potential study. One aspect that remains to be determined is the performance of mobile computing devices such as personal data assistants (PDAs) under this type of computational load.

Table 10 below describes the tasks to be accomplished during the exercise, as well the expected result, and a comments column that provides more detail on the accomplishment of each specific task.

Test Step	Expected Test Result	Comment	P/F
Test Description: This test veriefies that D-DACTs operating C2CE and transmitting over SecNet-11 cards with added MANET functionality can successfully inject PLI to the C2PC gateway.	**Expected Test Result**: D-DACTs will inject PLI information once every 60 seconds on the established interval, which will be successfully received by the C2PC gateway	**Test Objective**: Prove that Harris SecNet-11 wireless communications with added MANET functionality by CenGen can successfully inject PLI information to the C2PC gateway.	
STEP 1: Insert SecNet-11 card	Expected Response: D-DACT recognizes card and Ready Indicator light turns green	Card is recognized; validates sotware; properly installed.	Passed
STEP 2: Start-up OLSR by CenGen	Expected Response: Interface opens and the user is able to additional options Routes, Filters, multiple router discovery (MRD), etc.	Interface opens.	Passed
STEP 3: Select Routes by clicking the Routes button.	Expected Response: Route table inerface opens.	Click on routes and route table information is present. Default gateway is loopback address.	Passed
STEP 4: Refresh route table by clicking on Routes button.	Expected Response: After approximately five seconds, the routing table is updated. By clicking Routes button, the table is visually refreshed.	Default gateway now points to 172.25.1.129	Passed
STEP 5: Open up C2CE by slecting Start button and then selecting C2CE from the Start Menu.	Expected Response: C2CE application opens up.	C2CE version 6.0.13 is successfully initiated.	Passed
STEP 6: Start GPS services by clicking on the GPS icon from the C2CE menu bar.	Expected Response: GPS dialog box appears with the option to "Start GPS." When "Start GPS" is selected the screen changes and the system is attempting to get a position lock.	GPS is attempting to get position lock.	Passed
STEP 7: GPS receives and updates position from satellites and goes into navigation mode.	Expected Result: GPS icon changes from yellow (attempting to get posistion lock) to green "Navigating."	GPS icon turns green.	Passed
STEP 8: Repeat above steps for remaining three D-DACTs participating in the test.	Expected Results: Same as above. D-DACTS end up in "Navigating" mode.	Four D-DACTs now in "Navigating" mode.	Passed
STEP 9: Capture packets on D-DACT surrogate using Ethereal.	Expected Results: See PLI information from all four D-DACTs being delivered at 60-second intervals. (Setting configurable in C2CE options.	Ethereal shows PLI information being consistently delivered every 60 seconds.	Passed
Test Description: This test veriefies that D-DACTs operating C2CE and transmitting over SecNet-11 cards with added MANET functionality can successfully transmit and receive Chat traffic from all hosts in the network.	**Expected Test Result**: D-DACTs will receive and transmit Chat traffic to and from all hosts in the network through C2CE.	**Test Objective**: Prove that Harris SecNet-11 wireless communications with added MANET functionality by CenGen can successfully perform C2CE Chat functionality.	
STEP 10: Start Message Composer application of C2CE by clicking on the Signal Communicator icon from the C2CE menu bar.	Expected Response: Signal window opens.	Signal window opens successfully.	Passed
STEP 11: Select the comm check icon, which should deliver a message to all users on the network.	Expected Result: All D-DACTs, surrogate D-DACT and C2PC gateway receive comm check.	Comm check received by all stations.	Passed
STEP 12: Draft a message in the composer dialog box using the PocketPC keyboard.	Expected Results: Text is entered into the composer dialog box.	Message accepted and displayed in composer.	Passed
STEP 13: Click on Broadcast Transmit Icon in order to deliver the above message to all users on the network.	Expected Results: Message received by all D-DACTs.	Message successfully transmitted to all.	Passed
STEP 14: Repeat steps 8 and 9 from all D-DACTS to ensure proper dissemniation of all traffic.	Expected Results: Messages delivered and received among all users.	Message functionality works as designed.	Passed
STEP 15: Repeat steps 8 and 9 from the C2PC gateway to ensure Chat function delivers C2PC messages to C2CE hosts.	Expected Results: All traffic from C2PC gateway will be successfully delivered toal D-DACTs.	Message functionality works as designed.	Passed

Table 10. CenGen D-DACT Evaluation Task List

The testing at CenGen demonstrated the functionality of the C2CE application over the SecNet-11 SWLAN. PLI information was successfully delivered to the A Company gateway providing the common operation picture (COP) to all C2PC and C2CE clients; furthermore, the C2PC/C2CE chat function operated as designed.

This demonstration proved the value of mobile ad-hoc networking (MANET) to support mobile wireless clients by extending the lines of communication for IEEE 802.11b based SecNet-11 wireless cards. Two tests were performed to test the CenGen OLSR application. The first test involved the use of packet filters that disabled the delivery of datagrams to specific D-DACTs. The filters were applied on 1st Platoon's D-DACT so that it retained connectivity with the OLSR bridge and 2nd Platoon's D-DACT. 2nd Platoon's D-DACT retained connectivity with 1st and 3rd Platoon's D-DACT, and the 3rd Platoon's D-DACT retained connectivity only with 2nd Platoon. This manipulation forced the D-DACTs to select multi-point relays (MPRs) to forward datagrams for delivery.

The second test was performed outside the laboratory and required the operators to create sufficient physical separation between D-DACTs so that a "chain" was formed. This chain allowed for 1st Platoon's D-DACT to maintain radio frequency (RF) connectivity with the OLSR bridge and 2nd Platoon's D-DACT. 2nd Platoon's D-DACT retained RF connectivity with 1st and 3rd Platoon's D-DACT, and the 3rd Platoon's D-DACT retained RF connectivity only with 2nd Platoon. The CenGen OLSR application provided connectivity between these devices, despite the physical separation. All C2CE PLI traffic was successfully relayed back to the C2PC gateway and vice versa. Chat functionality among all clients was provided. Figure 76 shown below illustrates the "chain" created through packet filtering and physical separation.

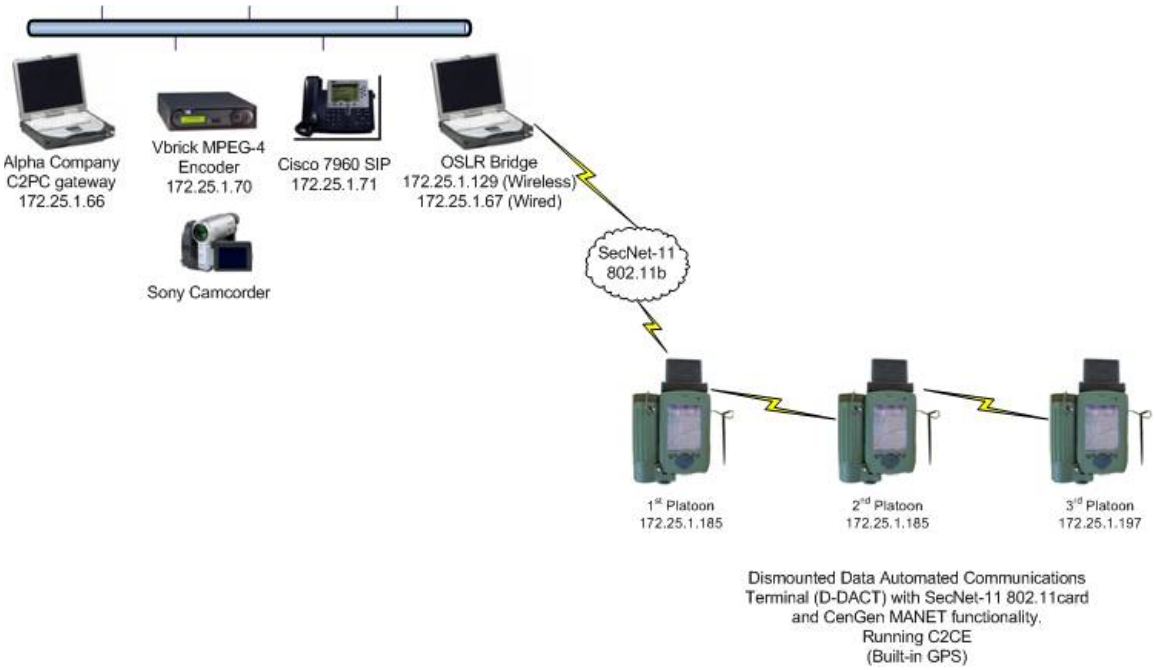

Figure 76. CenGen OLSR MANET Functionality Demonstration

These series of tests demonstrated the viability of a SWLAN for the D-DACT that could be integrated with IEEE 802.16 wide-area networking equipment for long distance backhaul.

4. D-DACT OLSR Configuration and SecNet-11 COMSEC (April 2005)

This third visit to southern California did not represent new experimentation but instead was an opportunity to acquire the pre-requisite tools in order to conduct further thesis research. Steven Durbano provided the CenGen OLSR application as well as the latest SecNet-11 drivers required for the creation of a SWLAN. Personnel at MCTSSA were able to provide an unclassified training fill for the SecNet-11 cards, which are inoperable until they receive COMSEC keying material.

Three D-DACTs were provided from Space and Naval Warfare (SPAWAR) Systems Center Charleston through coordination with Capt David Valentino the D-DACT Project Officer at Marine Corps Systems Command (MCSC). This suite of hardware and software combined with the assets in Mr. Rex Buddenberg's Internet-to-Sea Lab provided the necessary equipment and tools to conduct research.

C. SECNET-11 SWLAN AND REDLINE COMMUNICATIONS 802.16 POINT-TO-POINT LABORATORY TESTING WITH IXCHARIOT

1. Background

In this experiment, a baseline was established to determine the expected throughput a user could expect when using the SecNet-11 PCMCIA wireless cards to create a SWLAN and backhaul that traffic with Redline Communications 802.16 equipment. This experiment involved testing the basic connectivity and ensuring all of the equipment was functioning properly before conducting the experiments in the field environment. The basis for this experiment was to generate data that could be used to determine if the current proposed communication links from the Battalion down to the Platoon was a viable solution to obtain more bandwidth to the end user. IxChariot was used to capture the data for this experiment.

2. Network Architecture

The basic architecture for this lab experiment is shown in Figure 77 below.

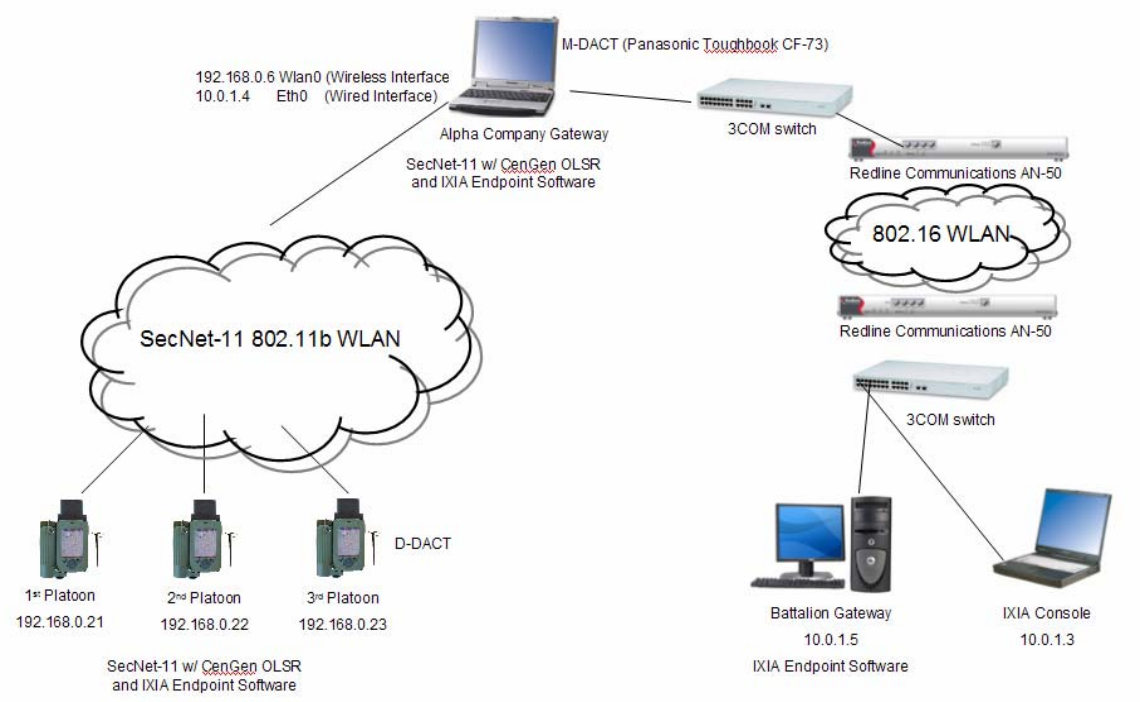

Figure 77. 802.11b/16 Lab Testing Experiment

In order to simulate what the communications link between a typical Battalion and Company would be, the AN-50's were bridges transmitting and receiving traffic to one another using the 802.16 protocol. Each AN-50 was wired into a 3COM switch that was connected to another computer, which simulated the C2PC gateway for the Battalion and Company.

The C2PC gateway on the Company side had a wired and wireless interface. The wireless interface could communicate with the three D-DACTs that were using the SecNet-11 wireless cards. This simulated the D-DACTs being assigned to each platoon commander in the field communicating back to the company. This link used the 802.11b protocol. Each device was loaded with Ixia's Performance Endpoint software to obtain data on the throughput.

3. Test Results

The test results from the lab experiment are shown below in Tables 11 through 16. Table 11 depicts the results obtained from sending the file send long benchmark script from the Ixia console, which emulated sending a 1 MB file from the BN GW to the Co GW wired interface on the uplink. This test was run in order to set a base for how much throughput a user could expect and if there was a difference between traffic flowing to the wired interface vice the wireless interface.

BN GW to Co GW (Wired Interface) Using 802.16				
End Point 1	End Point 2	Avg (Mbps)	Min (Mbps)	Max (Mbps)
BN GW	Co GW (Wired)	13.093	1.572	16.327
BN GW	Co GW (Wired)	14.107	1.563	16.327
BN GW	Co GW (Wired)	13.822	1.264	16.327
	AVG	13.674	1.466	16.327
	STDEV	0.523	0.175	0.000

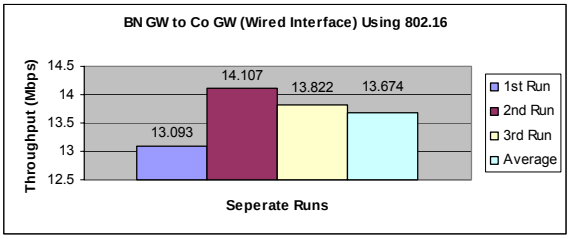

Table 11. BN GW to Co GW (Wired Interface) Using 802.16 and Corresponding Plot

The data obtained from the three tests showed an average throughput of 13.67 Mbps. The results of sending the traffic on the downlink are shown below in Table 12. The throughput measured from those three tests showed an average throughput of 15.94 Mbps.

Co GW (Wired Interface) to BN GW Using 802.16				
End Point 1	End Point 2	Avg (Mbps)	Min (Mbps)	Max (Mbps)
Co GW (Wired)	BN GW	15.94	15.385	16.327
Co GW (Wired)	BN GW	15.94	15.385	16.327
Co GW (Wired)	BN GW	15.924	15.094	16.327
	AVG	15.935	15.288	16.327
	STDEV	0.009	0.168	0.000

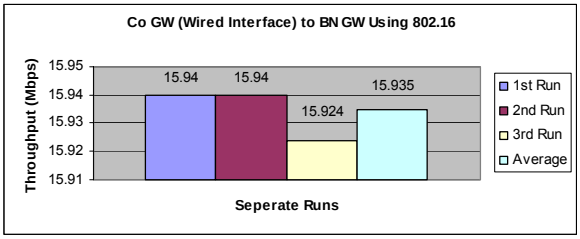

Table 12. Co GW to BN GW (Wired Interface) Using 802.16 and Corresponding Plot

Tables 13 and 14 shown below depict the results of sending the same data, but sending them through the wireless interface on the Co GW instead of the wired interface. As mentioned previously, sending data to the wired and wireless interface was done to test whether there was a significant difference in throughput that could be attributed to the OLSR bridging function.

BN GW to Co GW (Wireless Interface) Using 802.16				
End Point 1	End Point 2	Avg (Mbps)	Min (Mbps)	Max (Mbps)
BN GW	Co GW (Wireless)	13.378	1.268	16.327
BN GW	Co GW (Wireless)	14.766	1.713	16.327
BN GW	Co GW (Wireless)	14.636	1.556	16.327
	AVG	14.260	1.512	16.327
	STDEV	0.767	0.226	0.000

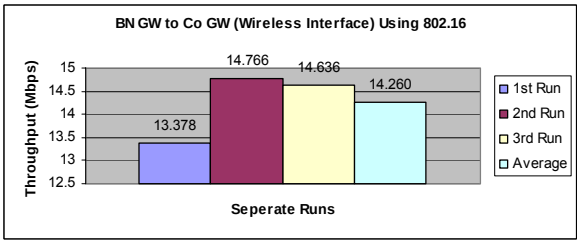

Table 13. BN GW to Co GW (Wireless Interface) Using 802.16 and Corresponding Plot

Co GW (Wireless Interface) to BN GW Using 802.16				
End Point 1	End Point 2	Avg (Mbps)	Min (Mbps)	Max (Mbps)
Co GW (Wireless)	BN GW	15.978	15.094	16.327
Co GW (Wireless)	BN GW	15.962	15.385	16.327
Co GW (Wireless)	BN GW	15.968	15.094	16.327
	AVG	15.969	15.191	16.327
	STDEV	0.008	0.168	0.000

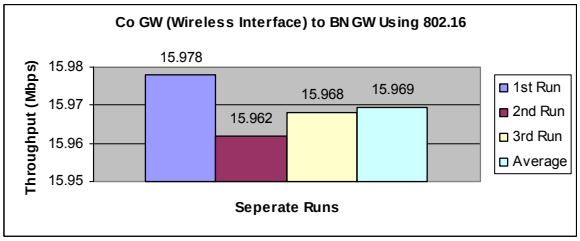

Table 14. Co GW (Wireless Interface) to BN GW Using 802.16 and Corresponding Plot

Tables 13 and 14 show average throughputs of 14.26 and 15.97 Mbps respectively. This was marginally higher than going through the wired interface, but not really a noticeable difference to the user. These values exceeded the throughput rates to

the wired interface; therefore, they failed to demonstrate a computational cost due to bridging the traffic from the wired network interface to the wireless SecNet-11 interface.

The next two tables depict data that traveled to and from the D-DACTs. Tables 15 and 16 below showed average throughput readings of 3.53 and 3.48 Mbps respectively.

BN GW to D-DACT Using 802.16				
End Point 1	End Point 2	Avg (Mbps)	Min (Mbps)	Max (Mbps)
BN GW	D-DACT 1	3.536	0.239	4.372
BN GW	D-DACT 2	3.497	0.237	4.324
BN GW	D-DACT 3	3.546	0.245	4.42
	AVG	3.526	0.240	4.372
	STDEV	0.026	0.004	0.048

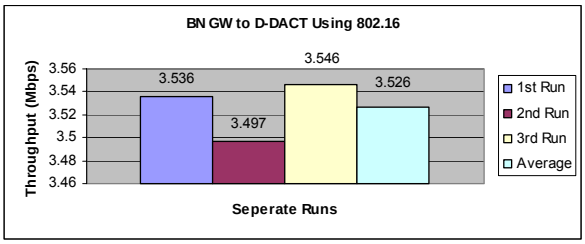

Table 15. BN GW to D-DACT Using 802.16 and Corresponding Plot

D-DACT to BN GW Using 802.16				
End Point 1	End Point 2	Avg (Mbps)	Min (Mbps)	Max (Mbps)
D-DACT 1	BN GW	3.519	2.073	3.721
D-DACT 2	BN GW	3.483	2.21	3.738
D-DACT 3	BN GW	3.451	1.869	3.738
	AVG	3.484	2.051	3.732
	STDEV	0.034	0.172	0.010

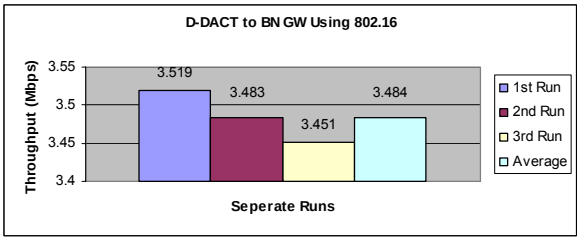

Table 16. D-DACT to BN GW Using 802.16 and Corresponding Plot

4. Summary

The results of the tests performed were useful in giving details of what to expect when testing the equipment in the field. The results above show that our assumptions of going through the Co GW wireless interface would be slower than going through the wired interface were faulty. The throughput was very similar with negligible differences. The most significant difference in throughput was noticed when IxChariot scripts were run from the console to the D-DACTs. The throughput of this test averaged 3.5 Mbps versus the 14 Mbps average over the 802.16 wireless links. The difference in throughput was expected as the clients of the SWLAN operated in a IEEE 802.11b ad-hoc network.

D. TACTICAL NETWORK TOPOLOGY FIELD EXPERIMENT (MAY 2005)

1. Background

The Tactical Network Topology (TNT) field experiments 05-3 were conducted at Camp Roberts Army National Guard Base in Paso Robles, CA, during May 2005. This

field exercise was used as the principal field test of this research. The focus of the exercise was two-fold. The first experiment would test throughput as a function of OLSR hop count. The second experiment would use Redline Communications' AN-50eFT manpack radio to provide a mobile wireless link for a Marine Corps rifle company. D-DACTs would communicate on a SecNet-11 SWLAN, and their C2CE traffic would be backhauled by the AN-50eFT to the Light Reconnaissance Vehicle (LRV). The LRV was used as a tactical Data Distribution System and established a wireless link to an AN-50e at the TOC. This wireless link allowed the Company C2PC gateway machine to deliver its PLI and Chat data to the Battalion C2PC gateway located inside Tactical Operations Center.

2. Throughput as a Function of OLSR Hop Count

For this exercise, eight D-DACTs and one Panasonic Toughbook CF-73 were used to create a SecNet-11 SWLAN. The Toughbook was used as a surrogate M-DACT and was configured to use dual interfaces. It used the wireless interface to participate in the SecNet-11 SWLAN and the wired interface to establish a connection to the TNT network via AN-50eFT manpack radio. Two AN-50e radios were collocated within the LRV. The first radio with IP address 192.168.98.30 established a wireless link with the AN-50eFT. This first radio was connected to a 3Com switch, which also had a Cat-5 connection with the second AN-50e in the LRV. This radio had an IP address of 192.168.98.21. The second radio established a wireless link with the AN-50e inside of the TOC. Figure 78 shown below illustrates the network used for this experiment.

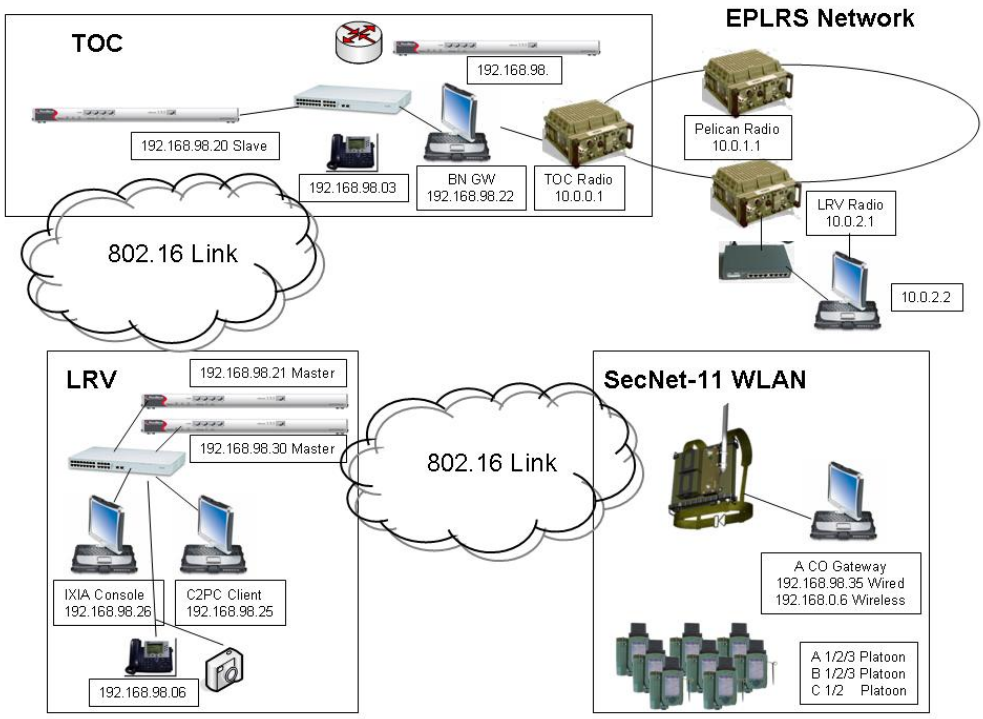

Figure 78. D-DACT SWLAN Throughput Experiment

The experiment used IXChariot, MGEN, and Netprobe to conduct network performance analysis to measure the effect on throughput, packet loss, and jitter, as the OLSR hop count was incremented by one. Packet filtering was used in order to increment the OLSR hop count through the same process described in Section B. "D-DACT Testing at CenGen and MCTSSA," of this chapter.

IxChariot throughput tests were configured to use TCP traffic and the File Send Long script. This script sends 100 timing records until they are completed. IXIA console was set up on a separate machine and tests were run in batch mode in order to offer the most accurate results. Figure 78 shown above illustrates the IXIA console machine connected to the 3Com switch in the LRV.

The first test established IXIA Console as End Point 1 and A Co 1st Plt as End Point 2. This test represents one OLSR hop. The network connectivity of this test required the IXIA console to traverse the 3Com switch to the AN-50e for transmission to

the AN-50eFT manpack radio. AN-50eFT radio traffic was first delivered to the A Company C2PC gateway, which served as an OLSR bridge for all the D-DACTs and then ultimately delivered to A Co 1st Plt. Subsequent tests increased the hop count by filtering the OLSR aloha packets, which required additional D-DACTs to relay the traffic. For example, Test 2 used IXIA Console as End Point 1 and A Co 2nd Plt as End Point 2; however, the 2nd Plt D-DACT was filtered so that it could receive traffic only from 1st Plt D-DACT, in effect forcing a second OLSR hop. This process was repeated until a total of nine hops were accomplished.

What was discovered by this series of experiments is that the loss of throughput due to increasing the OLSR hop count is well behaved. Figure 79 below shows throughput as a function of hop count. The nine-hop test labeled (spread out) means that this test was run with D-DACTs spread out across the McMillan Air Field in the vicinity of the TOC. This test was run twice as the first run failed to complete. (The first run is annotated with ***).

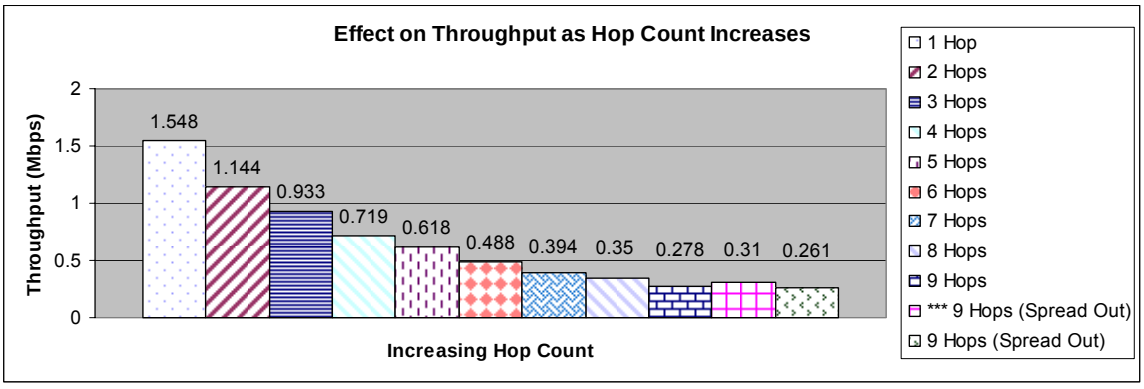

Figure 79. IXChariot Throughput Analysis as Hop Count Is Incremented

The Multi-Generator (MGEN) network performance test software was used to analyze the performance of the SWLAN with respect to packet loss, delay, and packet sequencing. For these experiments, MGEN was configured to send 512 byte-sized packets at a rate of 40 packets per second for a period of 60 seconds. Thus the generated bandwidth was

40 packets/second * 512 bytes/packet * 8 bits/byte * kbits/1000 bit) = 164 kbps

With a total number of packets generated being

60 sec * 40 packets/second = 2400 packets.

The 60-second run was performed at each hop count and packet loss was computed from the MGEN results. Figure 80 below is a plot graph that shows the packet loss percentage as a function of the number of hops. The results are well behaved up to five hops. After five hops, packet loss became an issue. What is shown with the subsequent NetProbe data is that after five hops, the NetProbe data began to spread more quickly (e.g. increased jitter). Based upon the combined results, one could hypothesize that no more than five hops may provide satisfactory data throughput. However, these results were obtained under advantageous network conditions (e.g. sitting together on a table). In a tactical environment where Marines are moving in and around structures, RF issues with signal interference will arise, and results may not be as clean, the acceptable hop count may be further reduced.

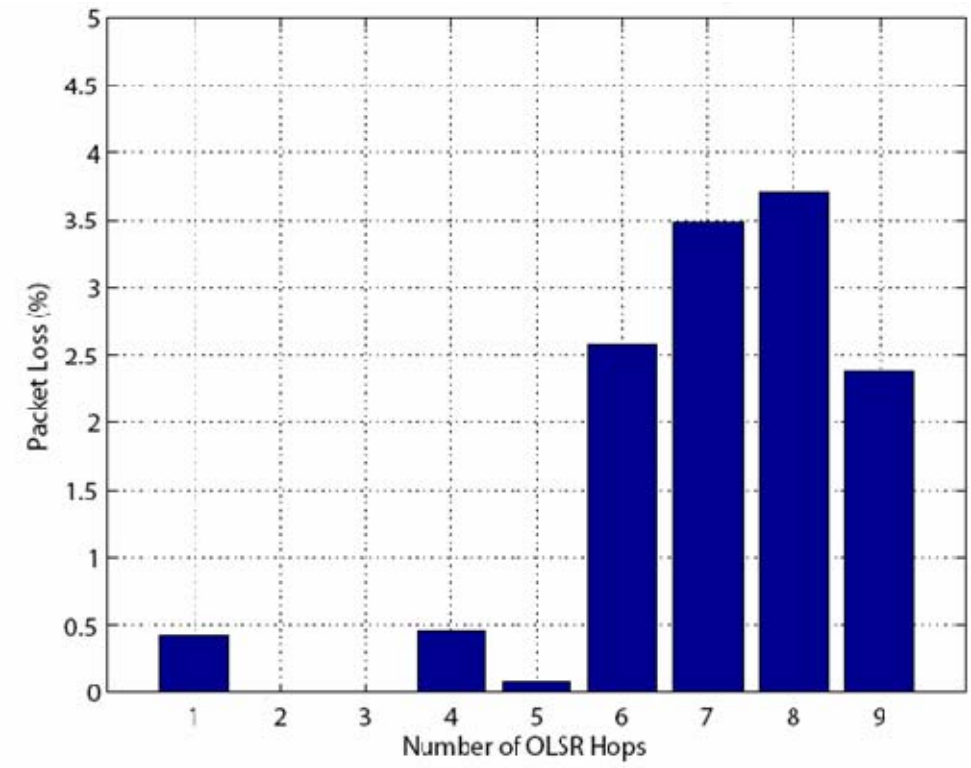

Figure 80. MGEN Packet Loss Analysis as Hop Count Is Incremented [31]

The NetProbe network monitor and protocol analyzer was used to measure the latency and jitter between two end points on a network. What the NetProbe data captured was a pattern of delay that increased as the number of hops increased. The actual delay values vary depending on the traffic load and other variables; however, each additional OLSR hop decreased the amplitude (frequency of occurrence) of the plot graph. For example, Figure 81 shown below has one high thin peak for the one-hop test; however, the peak diminishes in amplitude and widens as the number of hops increases. This affect is due to jitter. Jitter represents the difference in arrival times between successive NetProbe packets.

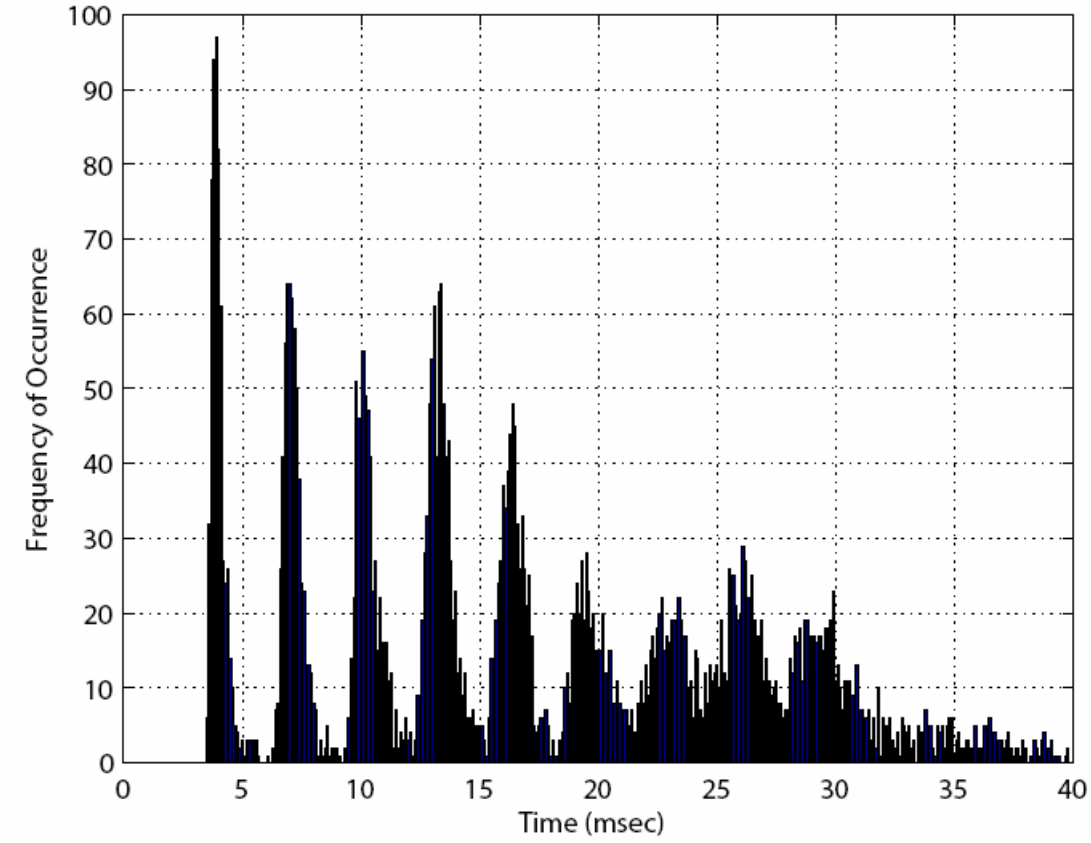

Figure 81. NetProbe Jitter Analysis as Hop Count Is Incremented [32]

This increased jitter as the number of hops increases can cause significant problems for real-time data streams such as streaming video and Voice over Internet Protocol (VoIP). It can also reduce TCP performance, which is evidenced by the IxChariot TCP shown above in Figure 79. A follow-on test that would have produced

valuable data here would have been to run some qualitative measurements of actual streaming video and VoIP traffic. The degradation in performance would have been quite clear, as evidenced through video quality and audio quality, respectively.

This jitter analysis has significant implications as the effect of increased jitter is a major determining factor with respect to performance attributes of a MANET network. These series of tests demonstrate that the OLSR protocol (or any other MANET protocol) is capable of route and delivery, yet this functionality alone does not infer that the application data will pass through the MANET network without problems. For real-time streaming applications and TCP applications there is a limit to the number of hops that can be traversed before the application is considered unusable.

Much work is being done to improve data throughout in tactical environments where packet loss, latency and jitter are serious concerns. Reliable transport protocols and ad-hoc protocols (e.g. ad-hoc TCP) are some areas of investigation that should be reviewed to determine their maturity and application to military networks.

3. AN-50eFT Mobile Wireless Link

This scenario was designed to provide connectivity similar to that of the tactical Internet. Platoon D-DACTs would communicate using the SecNet-11 SWLAN similar to the connectivity achieved with the AN/PRC-119 SINCGARS radio. The AN-50eFT manpack radio would provide wide-area communications similar to the EPLRS radio. Figure 82 shown below illustrates operationally the network used to execute this experiment.

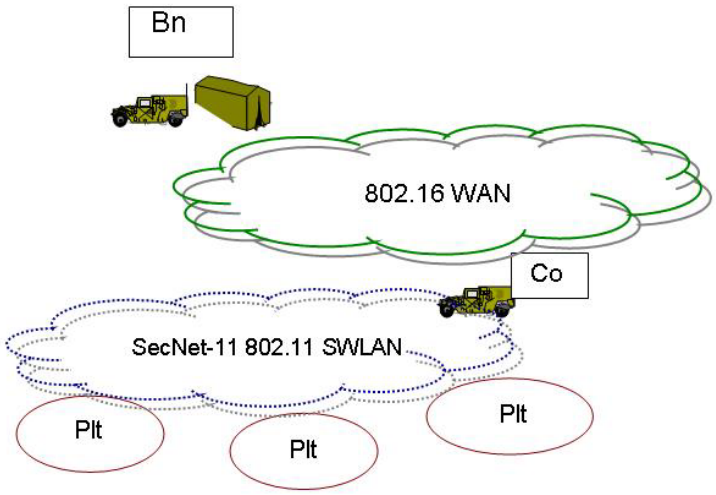

Figure 82. SWLAN D-DACT Connectivity and IEEE 802.16 Wireless Backhaul

As in Experiment 1 described above, this next experiment used eight D-DACTs and one Panasonic Toughbook CF-73 to create a SecNet-11 SWLAN. The Toughbook was used as a surrogate M-DACT and was configured to use dual interfaces. It used the wireless interface to participate in the SecNet-11 SWLAN and the wired interface to establish a connection to the TNT network via the AN-50eFT manpack radio. Two AN-50e radios were collocated within the LRV. The first radio with the IP address 192.168.98.30 established a wireless link with the AN-50eFT. Figure 83 below shows the rear of the LRV with its equipment rack. The upper An-50 was used to establish a wireless link to the AN-50eFT.

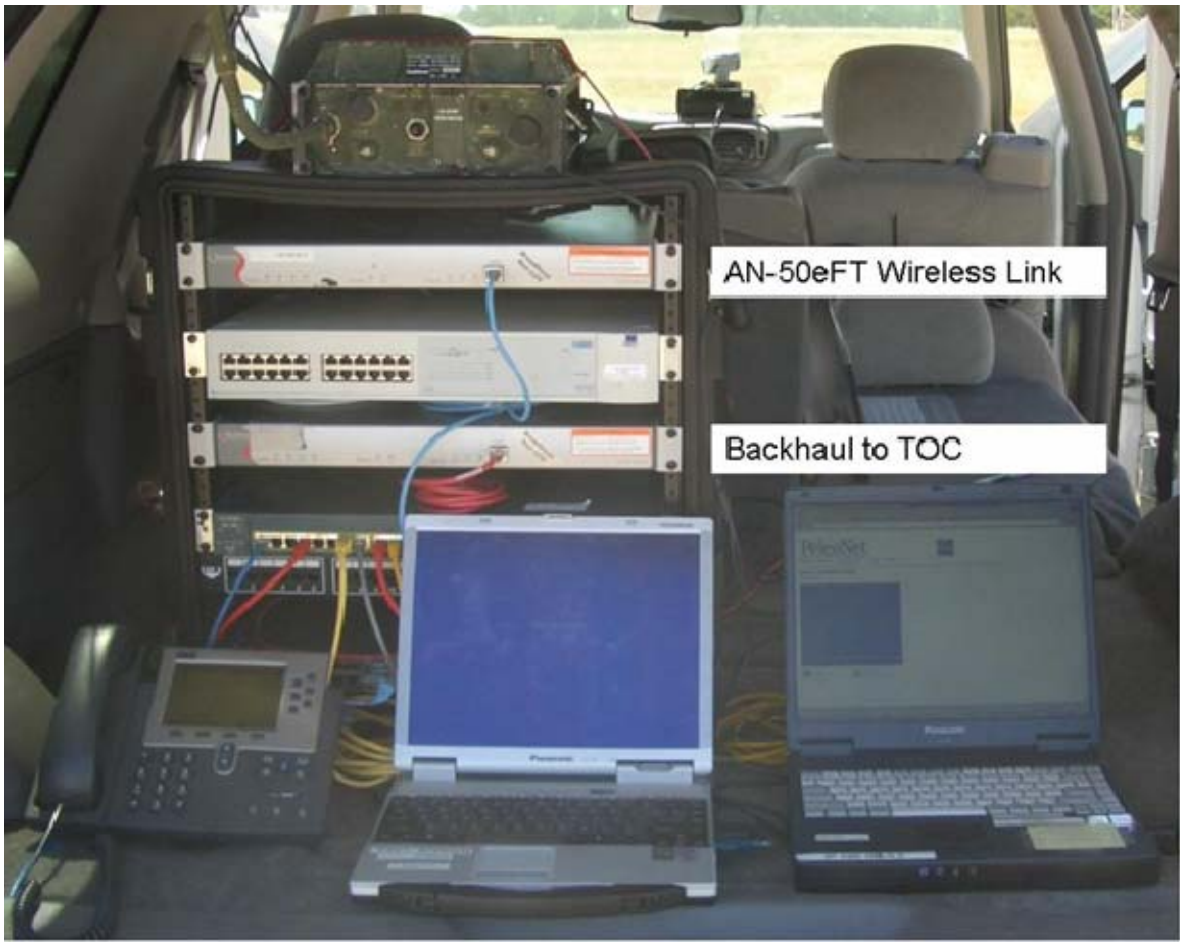

Figure 83. Light Reconnaissance Vehicle Redline 802.16 Suite

The upper radio was connected to a 3Com switch, which also had a Cat-5 connection to the second AN-50e in the LRV. The second radio had an IP address of 192.168.98.21. This second radio was used to establish a wireless link with the AN-50e inside of the TOC. The upper radio in the LRV used a 9 dBi omni-directional antenna to establish a wireless link to the AN-50eFTmanpack radio. The lower radio in the LRV used a 90° sector antenna with 17 dBi to establish the wireless link to the AN-50e at the TOC. Figure 84 below shows the antennas mounted to the top of the LRV.

Figure 84. Light Reconnaissance Vehicle with Omni-Directional and Sector Antenna

As mentioned previously, in this section all eight D-DACTs were all connected to a Panasonic Toughbook CF-73 running C2PC Gateway. The Toughbook was a surrogate for the Company Commander's Mounted Data Automated Communications Terminal (M-DACT), and this hierarchical connectivity is consistent with Marine Corps Standard Operating Procedures (SOPs), though a more accurate architecture would have provided for Bravo and Charlie Company C2PC gateways. (This architecture was selected based on personnel and gear requirements). This hierarchical connectivity allows for efficient transmission of all Position Location Information (PLI) from platoon to battalion and supports equitable taxation of Gateway machines. PLI reports from the D-DACTs are all delivered to the Company Gateway at one-minute intervals and delivered from the Company Gateway to Battalion Gateway at a user configurable interval (typically 30 seconds). Figure 86 below shows the tracks present at the A Company C2PC gateway as of 1634 on the 24th of May 2005.

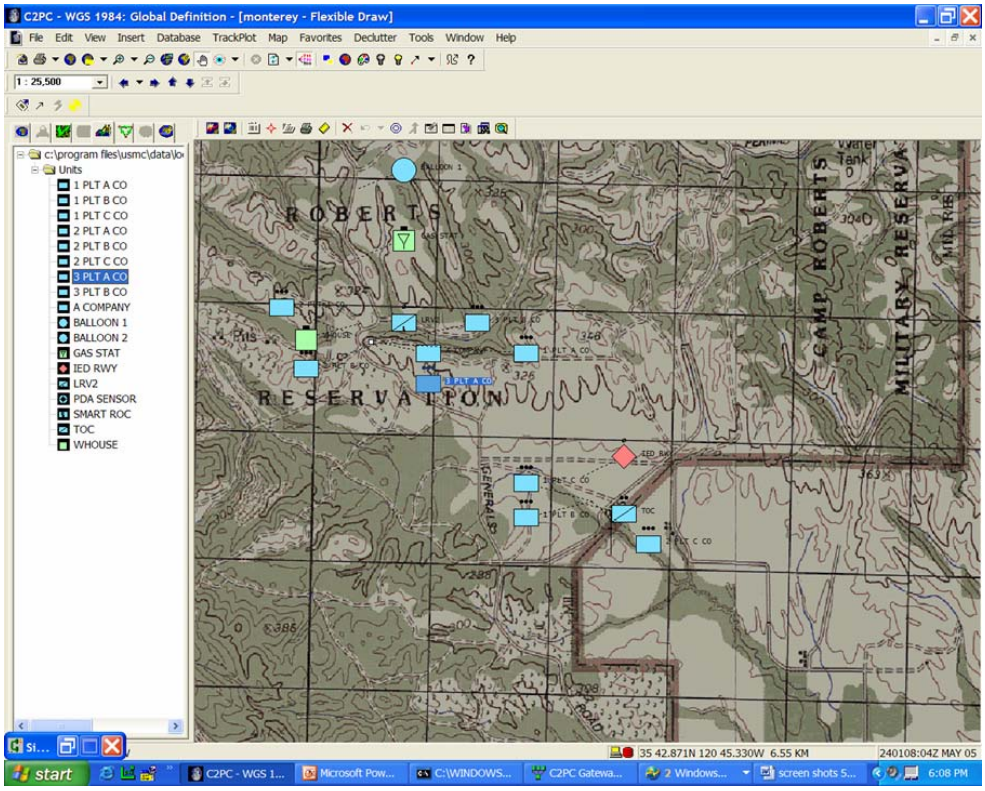

Figure 85. Common Operational Picture at the Company Gateway at 1634 24 May 2005

During Experiment 2, the common operational picture (COP) was slow to refresh among the distributed clients. C2PC clients seldom displayed the green "synched" icon but routinely displayed the yellow "synching" icon. This meant that the clients were successfully connected to their respective C2PC gateway machines but were unable to synchronize the COP. Due to the time constraints of the exercise, this synchronization issue was not fully explored. This scenario was not duplicated in the laboratory environment.

In addition to testing the PLI injection feature of C2CE/C2PC, we tested the built-in chat function. The chat function allows for near real-time transfer of text data. This feature allows commanders to issue immediate short orders or other relevant information. Microsoft NetMeeting was tested over the Redline 802.16 wireless link to use its chat

feature. Lastly, Internet Relay Chat (mIRC) chat was established between the D-DACTs and the C2PC gateway machine in the TOC, which was running the mIRC server software.

4. TNT Field Experiment 05-3 Summary

The ability to perform these two experiments during TNT 05-3 was a unique opportunity. This was the first time that nine OLSR hops had been tested to see the effect upon throughput, packet loss, and jitter. Secondly, integration with the LRV provided an excellent opportunity to use IEEE 802.11b and 802.16 wireless technologies in a notional tactical deployment. The LRV successfully accomplished its role as a tactical DDS as 802.16 links from the manpack radio to the LRV were readily established, and the 802.16 link from the LRV to TOC was solid throughout the exercise. Traffic from the SecNet-11 WLAN was successfully back-hauled to the TOC, though these tests should be repeated in order to ensure the optimal configuration of C2PC gateways to ensure a more timely synchronization of the CTP.

E. SECNET-11 SWLAN AND REDLINE COMMUNICATIONS 802.16 POINT-TO-MULTI-POINT LABORATORY TESTING WITH IXCHARIOT (SEPT 2005)

1. Background

All experiments up to this time had used the Redline Communications AN-50e devices in point-to-point mode (PTP). This mode of operation can be used to support specific mission requirements; however, a review of this technology would be incomplete without analyzing point-to-multi-point (PMP) operations. PMP mode allows a single AN-50e that has the base station software loaded to service multiple SSs. Thus testing, from this point forward, used the PMP functionality of the Redline equipment.

The operational scenario for this test was designed around a Marine infantry battalion. Current techniques, tactics, and procedures (TTP) call for communications equipment to be physically separated from the combat operations center (COC) and located on advantageous terrain. The purpose is two-fold: first, all communications equipment emits electromagnetic energy that can be detected and its source can be triangulated. Thus physical separation from the COC provides some measure of protection from discovery or targeting by enemy personnel. Secondly, communications

assets are located on advantageous terrain in order to improve line-of- sight variables, such as higher elevation, less foliage, etc. Therefore, the AN-50e base station would be collocated with organic communications assets and remoted into the COC.

The AN-50e at the battalion would require the use of either an omni-directional antenna or a sector antenna with a wide azimuth to service several SSs in a field environment. Figure 86 below illustrates a conceptual model for servicing a battalion's three rifle companies.

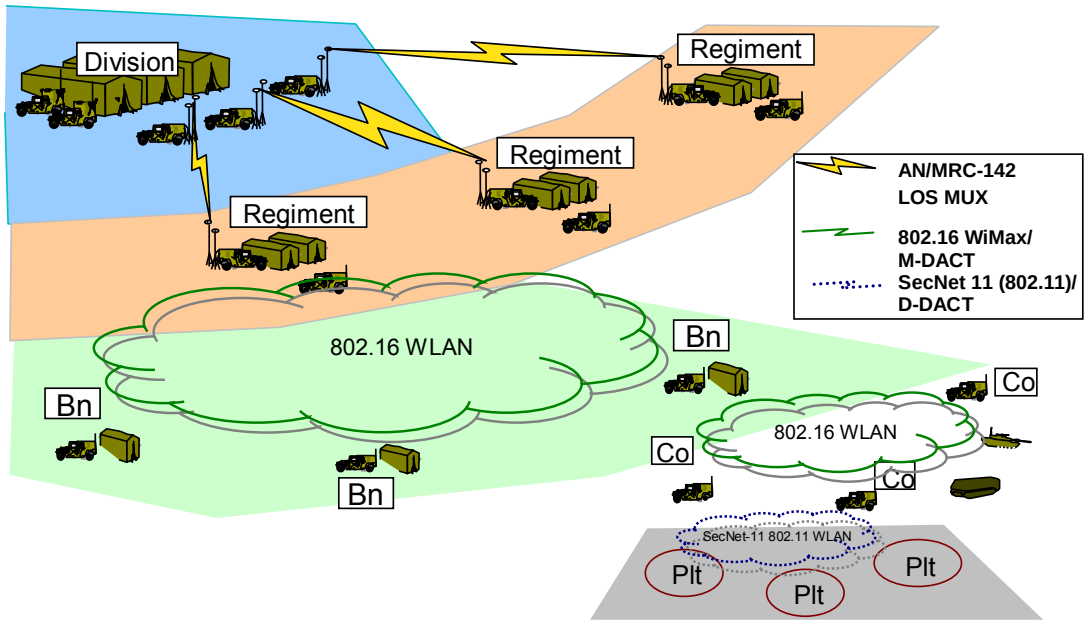

Figure 86. Proposed SWLAN with Redline AN-50e Point-to-Multi-Point Operation

Each rifle company would require their own individual AN-50e device to communicate with the base station located at the battalion. Base stations can support more than three SSs; however, due to equipment and personnel limitations, this research used a total of four AN-50e radios. One configured as the base station and three configured as SSs. The deployment of the four AN-50e radio supports the operational schematic shown above in Figure 86. These experiments were designed to test the effect on throughput as the numbers of SSs associated to the single base station were increased.

Redline Communications' implementation of the IEEE 802.16 standard adopted Time Division Duplex (TDD) transmissions; therefore, the composite frame is divided into three sections. The first is used strictly by the base station in order to administer the wireless network. The second frame is the maintenance queue, which allows for SSs to access the medium and perform the tasks necessary to associate to the base station. The third frame provides transmit slots to the SSs. Figure 87 below illustrates the IEEE 802.16 composite frame for systems using TDD.

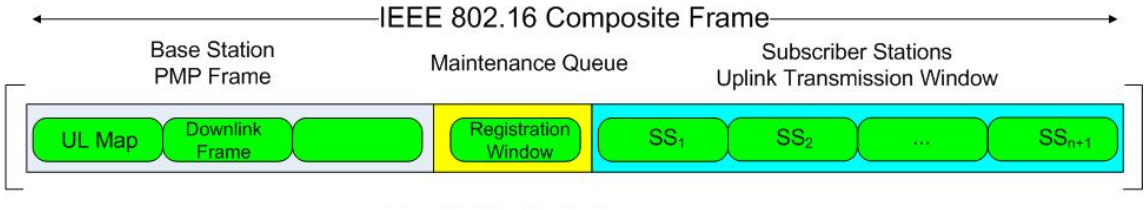

Figure 87. IEEE 802.16 Composite Frame for TDD Systems Adapted from IEEE 802.16.3c-01/33r2 "OFDM Proposal for the IEEE 802.16a PHY Draft Standard" [33]

2. Network Architecture

The network architecture designed for this experiment used three AN-50e units that were mounted in a 19-inch rack. Each AN-50e SS represented a radio required by each company commander to establish a wireless link to the base station, as depicted above in Figure 87. The range within the laboratory between these Redline Communications devices was approximately 20 feet. Therefore, the transmit power on all AN-50e radios was set to -10 dBm to avoid damaging the equipment with excessively powerful received signal strength. Each AN-50e used a Wi-Fi Plus, 40° multi-polar sector antenna that had 17 dBi of gain, as shown in Figure 88 below.

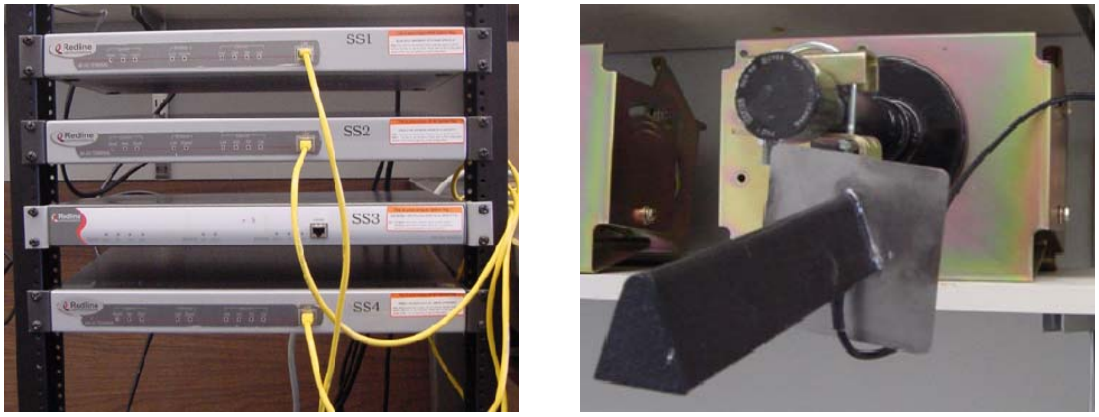

Figure 88. AN-50e Subscriber Stations and 40° Sector Antenna in the Laboratory

Each SS had a Panasonic Toughbook CF-48 attached via Cat-5 cable. These CF-48 machines simulated a company commander's M-DACT connected to its assigned AN-50e. SS 1 serviced the A Co C2PC gateway machine, SS 2 serviced B Co, and SS 3 serviced the C Co machine. All network devices were assigned IP addresses within the same sub-network and routers were not employed. Each CF-48 had IXIA end point software installed.

Across the room from the SSs, the BS was mounted in its own 19-inch rack. The BS used a 12 dBi omni-directional antenna in order to provide connectivity to all three SSs. Figure 89 below shows the BS and its omni-directional antenna.

Figure 89. AN-50e Base Station and Omni-Directional Antenna in the Laboratory

The BS was connected to the 3Com switch shown in Figure 89 above. Port number one on the 3Com switch received a Cat-5 cable that was connected to an Ethernet

wall drop providing connectivity to the Naval Postgraduate School's network. This extended Internet connectivity to all the nodes hanging from their respective SSs. The switch was also connected to a Dell Optiplex GX 270 desktop. For these experiments, the Dell served as the battalion C2PC gateway machine. A Panasonic Toughbook CF-48 was connected to the switch as well in order to host the IXChariot console software. The IXChariot File Send Long benchmark script was used to perform TCP traffic analysis.

3. Test Results

a. Experiment #1

The first experiment used the IXChariot Console to test the throughput from the CF-48 corresponding to A Company to the Dell desktop, which was configured as the battalion C2PC gateway machine. The same IXChariot script was used three separate times as additional SSs were brought online and associated to the BS. Therefore, the first run executed the IxChariot script while one SS was online. The second run had two SSs, and the third run had three SSs. Table 17 below lists the separate runs as well as a test average. Figure 90 is its corresponding graph.

A Co GW (Wired Interface) to BN GW Using 802.16					
End Point 1	End Point 2	Active SS	Avg (Mbps)	Min (Mbps)	Max (Mbps)
A Co (Wired Interface)	BN GW	1	10.938	1.268	16.327
A Co (Wired Interface)	BN GW	2	7.639	1.244	13.333
A Co (Wired Interface)	BN GW	3	9.25	1.067	11.268
	AVG		9.276	1.193	13.643
	STDEV		1.650	0.110	2.544

Table 17. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Test

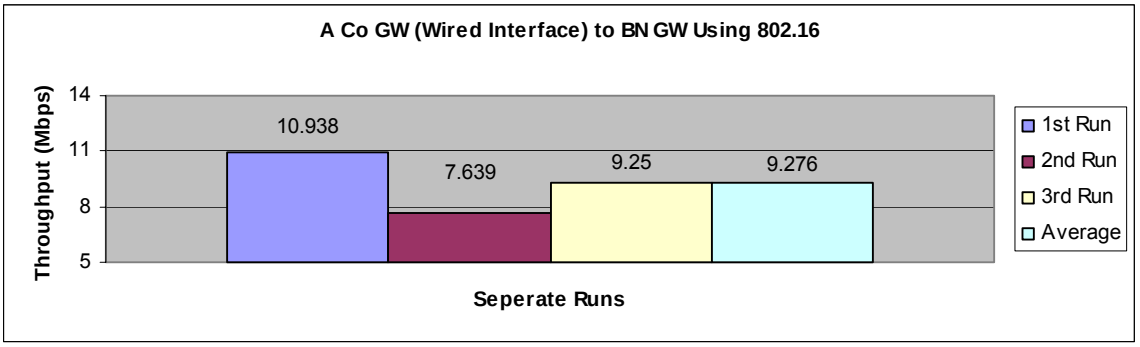

Figure 90. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Plot

The data obtained from this test showed an average uplink throughput of 9.276 Mbps. This test was repeated and the values for the second run are in Table 18 and Figure 91.

A Co GW (Wired Interface) to BN GW Using 802.16 2nd Run					
End Point 1	End Point 2	Active SS	Avg (Mbps)	Min (Mbps)	Max (Mbps)
A Co (Wired Interface)	BN GW	1	12.085	1.272	16.327
A Co (Wired Interface)	BN GW	2	8.917	1.473	13.333
A Co (Wired Interface)	BN GW	3	8.487	1.252	11.111
	AVG		9.830	1.332	13.590
	STDEV		1.965	0.122	2.618

Table 18. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Test (2nd Run)

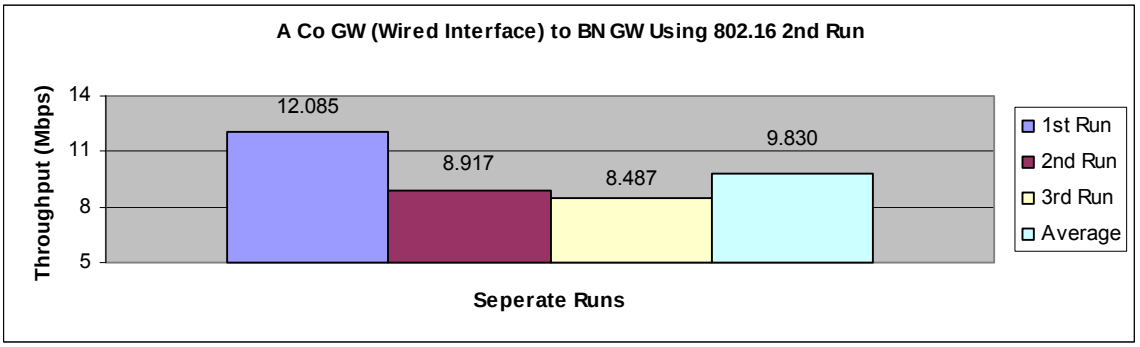

Figure 91. A Co C2PC Gateway to BN C2PC Gateway IxChariot Throughput Plot (2nd Run)

b. Experiment #2

In order to test the downlink, the same test scenario as described in Experiment 1 above was repeated with the exception that the Dell desktop (battalion C2PC machine) was configured as End Point 1, and A Co C2PC gateway became End Point 2. Once again, three separate runs were executed. For the first run, one SS was associated, for the second run, two SSs were associated, and for the third run, three SSs were associated. The data obtained from this test returned an average downlink throughput of 11.588 Mbps. Table 19 and Figure 92 below show the results of these tests.

BN GW to A Co GW (Wired Interface) Using 802.16					
End Point 1	End Point 2	Active SS	Avg (Mbps)	Min (Mbps)	Max (Mbps)
BN GW	A Co (Wired Interface)	1	12.981	11.111	13.333
BN GW	A Co (Wired Interface)	2	10.731	9.091	11.268
BN GW	A Co (Wired Interface)	3	11.053	10.39	11.268
	AVG		11.588	10.197	11.956
	STDEV		1.217	1.024	1.192

Table 19. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Test

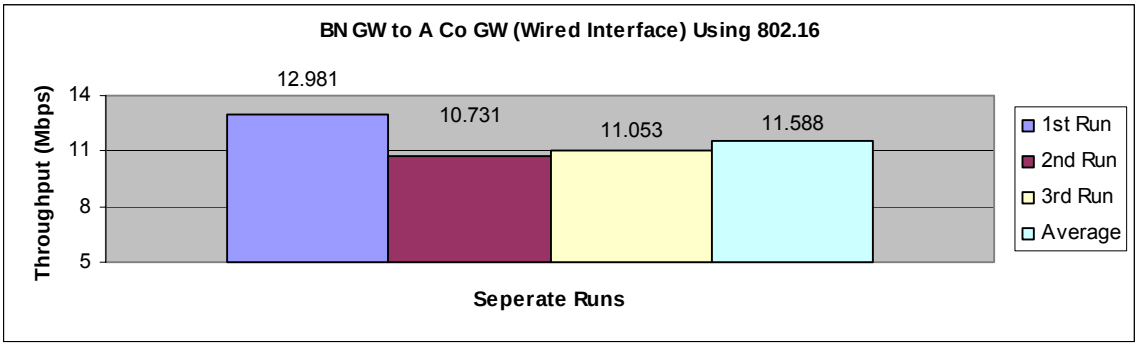

Figure 92. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Plot

This downlink test was repeated, and the values for the second set of tests are shown below in Table 20 and Figure 93.

BN GW to A Co GW (Wired Interface) Using 802.16 2nd Run					
End Point 1	End Point 2	Active SS	Avg (Mbps)	Min (Mbps)	Max (Mbps)
BN GW	A Co (Wired Interface)	1	12.998	11.111	13.559
BN GW	A Co (Wired Interface)	2	10.741	9.091	11.268
BN GW	A Co (Wired Interface)	3	11.051	10.127	11.268
	AVG		11.597	10.110	12.032
	STDEV		1.223	1.010	1.323

Table 20. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Test (2^{nd} Run)

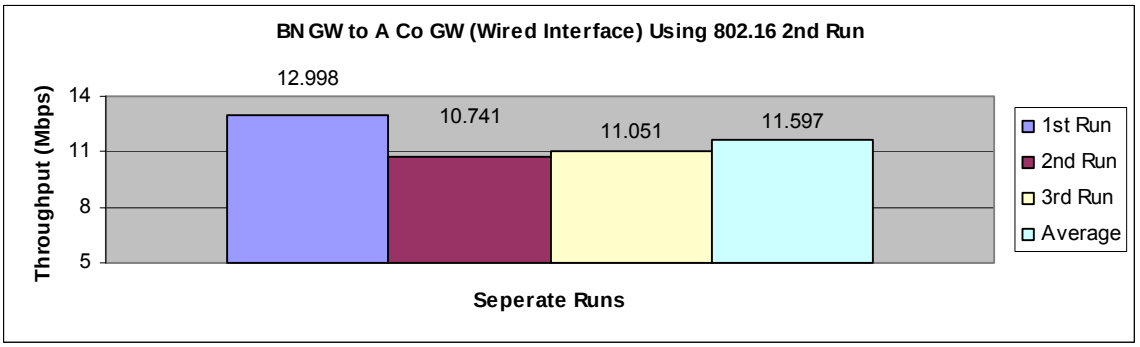

Figure 93. BN C2PC Gateway to A Co C2PC Gateway IxChariot Throughput Plot (2nd Run)

4. Summary

These tests failed to prove that throughput decreases as additional SSs are associated to a single BS. Several factors led to these tests being inconclusive. The most critical is that an insufficient number of SSs were associated to the BS. The effect of three SSs sharing the allotted portion of the IEEE 802.16 composite frame was not significant. To run this experiment conclusively, a sufficient number of SSs to reach system failure, signifying that the BS has exceeded its capacity to service SSs are required. Through an exchange of e-mail with a Redline Communications technical representative, it was established that a single BS can service a total of 20 SSs based on the current implementation.

A second factor was insufficient computation load upon the wireless system. The SSs only hosted a single computer and each of these machines only ran the C2PC application during the test. The Redline 802.16 equipment dynamically redistributes time slots to SSs as needed, therefore, the stations performing low bandwidth tasks receive smaller fractions of the SSs uplink transmission window.

A final factor is the radio frequency conditions within the small enclosed laboratory environment were not ideal for the execution of this test and caused unfavorable background noise.

F. SECNET-11 SWLAN AND REDLINE COMMUNICATIONS 802.16 POINT-TO-MULTI-POINT FIELD EXPERIMENT (SEPT 2005)

1. Background

This section covers the point-to-multi-point (PMP) test conducted at Fort Ord, CA. The operational scenario for this test was designed around the communications structure of a Marine infantry battalion. Consequently, the test used the same network architecture as described in Section E of this chapter. Three SSs were again associated to the BS and one CF-48 laptop was connected to each SS. The BS had two laptops connected to it: the battalion C2PC gateway and the IxChariot console machines. Figure 94 below illustrates the network used for this experiment.

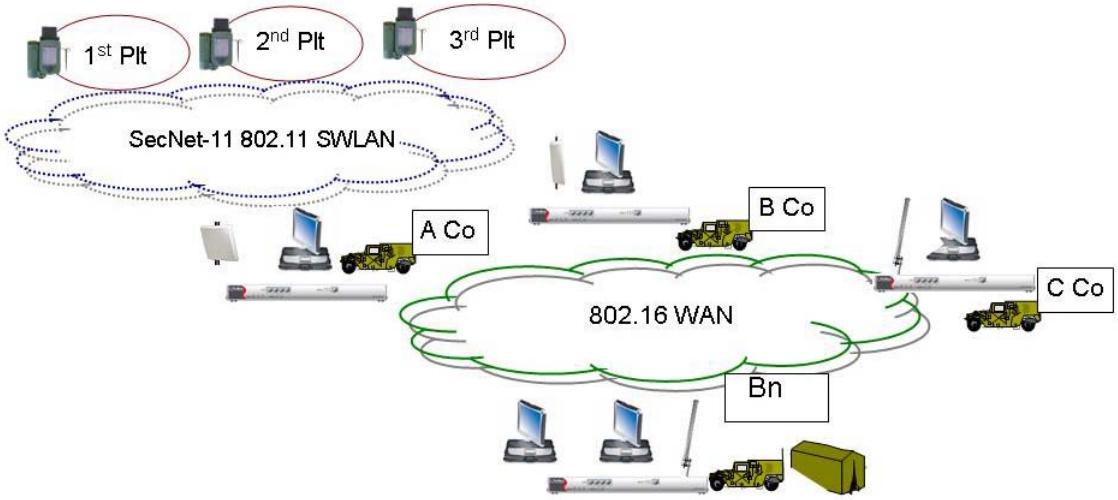

Figure 94. Fort Ord Point-to-Multi-Point Network Architecture

2. Network Architecture

The BS used a 12 dBi omni-directional antenna mounted atop an antenna mast raised to 15-feet to service the three SSs. SS 1, which corresponds to A Co as shown in Figure 94 above, used a one-foot flat panel antenna raised on an antenna tripod to an elevation of six feet. SS 2, which corresponds to B Co used a 40° sector antenna with 17 dBi of gain, and was mounted on an antenna tripod to a height of six feet. Lastly, SS three belonging to C Co used a 9dBi omni-directional antenna and was raised to a height

of six feet on an antenna tripod. GPS was used to obtain an accurate measurement from the BS, and each SS had clear line of sight to the BSs antenna. The GPS coordinates and antenna type for each AN-50e are shown in Table 21.

Fort Ord Point-to-Multi-Point Throughput Testing				
	Base Station	**SS #1**	**SS #2**	**SS #3**
Assigned Role	Bn BS	A Co SS	B Co SS	C Co SS
GPS Position	10S FF 13141 57125	10S FF 13261 56930	10S FF 13029 56946	10S FF 12907 57158
Distance from BS (meters)	N/A	230m	210m	230m
Antenna Type	12 dBi Omni-directional	22 dBi 1' flat panel	40° sector 17 dBi	9 dBi Omni-directional
Computer Hosts	BN C2PC Gateway Ixia Console	A Co C2PC Gateway	B Co C2PC Gateway	C Co C2PC Gateway

Table 21. AN-50e Radio Deployment Characteristics

The A Co CF-48 was configured as an OLSR bridge and used dual interfaces to participate in the SWLAN and to transmit information over the 802.16 radio WAN. Two D-DACTs were deployed in the vicinity of the A Co position and together with the A Co laptop comprised the SWLAN.

The three company computers had C2PC installed, and all three were connected to the battalion C2PC gateway machine. Moreover, all three were GPS enabled through a serial cable connection to a Garmin Rhino 110 GPS receiver. The two D-DACTs had C2CE installed and were connected to the A Co C2PC gateway machine. The D-DACTs were GPS enabled. All computers on the network had IxChariot End Point software installed.

3. Test Results

The test consisted of running nine individual IxChariot scripts among the clients in the WAN. Tests could not be completed to C Co due to Symantec Client Firewall issues that prevented the Ixia console from initiating the TCP script with this terminal. The file send long benchmark test was used for these tests. Table 22 shows the results of each of the nine runs, as well as the average.

Fort Ord Point-to-Multi-Point IxChariot Throughput Analysis					
End Point 1	End Point 2	Active SS	Avg (Mbps)	Min (Mbps)	Max (Mbps)
A Co (Wired Interface)	B Co	3	8.603	8.000	8.791
A Co (Wired Interface)	BN GW	3	8.107	1.046	11.268
A Co (Wired Interface)	Ixia Console	3	11.105	10.526	11.268
B Co	A Co (Wired Interface)	3	7.131	5.442	8.511
B Co	BN GW	3	6.834	1.117	10.390
B Co	Ixia Console	3	8.302	6.299	10.959
Bn GW	A Co (Wired Interface)	3	11.036	10.390	11.268
Ixia Console	A Co (Wired Interface)	3	11.104	10.390	11.268
Ixia Console	B Co	3	10.998	10.127	11.268
	AVG		9.247	7.037	10.555
	STDEV		1.805	3.859	1.119

Table 22. Fort Ord Point-to-Multi-Point IxChariot Throughput Test Results

The results of the tests provide only one discernable pattern, which is that higher throughput values were observed during downlink versus uplink tests. For example, a review of the tests in which End Point 1 was either the BN Gateway or the Ixia console, higher throughput values were recorded. These two machines were connected to the BS. Figure 95 is a plot graph with the results of the tests run at Fort Ord.

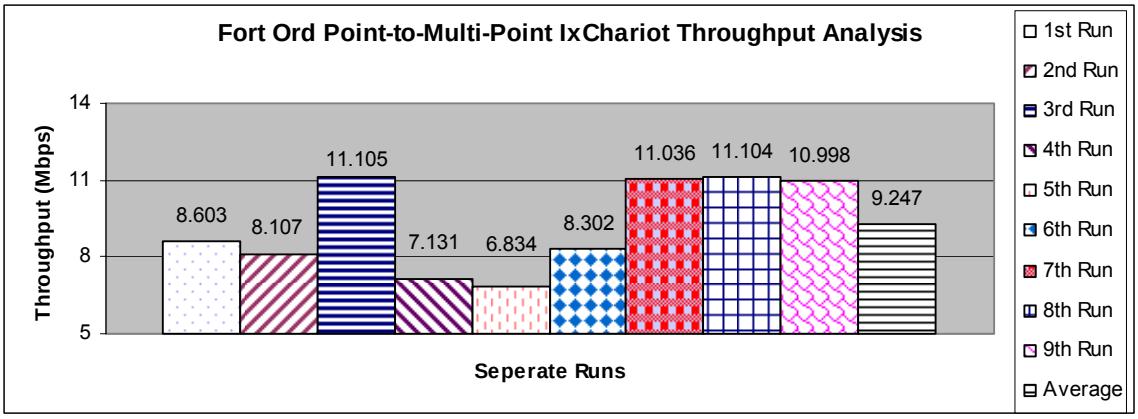

Figure 95. Fort Ord Point-to-Multi-Point IxChariot Throughput Plot

4. C2PC Functionality

As mentioned in Section 2 of this experiment, the C2PC and C2CE applications were running on the CF-48 laptops and D-DACTs. The PLI and Chat features of these devices were tested to ensure operability across a point-to-point radio WAN. The C2PC

application worked as designed, and the clients were able to connect to their respective C2PC gateway. The COP was populated by tracks from the GPS enabled devices. Figure 96 shown below is a screen capture from the A Co computer taken at 1630 2 Sept 2005.

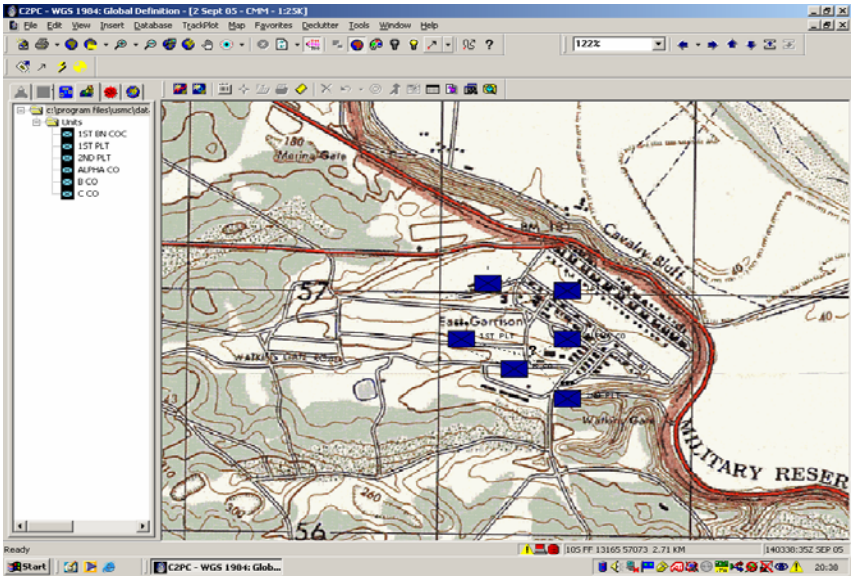

Figure 96. C2PC Screen Capture from A Co Gateway at 1630 2 Sept 2005

5. Summary

The point-to-multi-point tests run at Fort Ord, CA, captured throughput analysis for a deployment of three SSs. The results from this outdoors deployment returned throughput values of 6.834 Mbps to 11.105 Mbps. The results achieved warrant further analysis in order to determine whether the same deployment would return similar results; however, these tests at Fort Ord were the last opportunity to use this gear as it was embarked the following day with a 15-member detachment of Naval Postgraduate School students who deployed to Waveland, MS, in support of hurricane-relief operations.

These tests failed to prove that throughput decreases as additional SSs are associated to a single BS. Several of the items described in the summary from Section E of this chapter, were evident in this series of tests. The most important item is that an insufficient number of SSs were associated to the BS. The effect of three SSs sharing the allotted portion of the IEEE 802.16 composite frame was not significant. To run this

experiment conclusively, a sufficient number of SSs to reach system failure, signifying that the BS has exceeded its capacity to service SSs are required.

A second factor was insufficient computation load upon the wireless system. The SSs only hosted a single computer and each of these machines only ran the C2PC application during the test. A more appropriate test should analyze throughput under more realistic network conditions.

VI. ADAPT FROM COMMERCIAL-OFF-THE-SHELF (COTS) RECOMMENDATIONS

A. INTRODUCTION

Though several communication requirements within the Marine Corps can leverage this technology as it exists today, this chapter examines the potential adaptations to the IEEE 802.16 standard and WiMAX compliant equipment that would make these technologies viable to a larger percentage of military users. Of particular interests to this study is a means to adapt these technologies to small mobile units that today use the tactical Internet to support their warfighting functions.

B. ADAPT FROM COMMERCIAL-OFF-THE SHELF

1. Physical Layer

a. Frequency

Chapter III of this thesis presented the current radio assets employed by the MAGTF to describe how those assets rely upon frequencies at the lower end of the electromagnetic spectrum. Military communication systems predominately use frequencies between 3 MHz and 400 MHz encompassing HF, VHF, and UHF bands. These frequency bands were selected because they presented properties advantageous to mobile forces, who routinely operate in non-line-of-sight environments.

The IEEE standard leverages the unlicensed ISM band between the ranges of 2 GHz and 66 GHz. Though several military communication requirements can leverage that band of frequencies (the LSWAN program described in Chapter IV is one example) most military users cannot. Adapting the IEEE 802.16 protocol to varied frequency bands is allowed by the independence of the physical and data link layers of the protocol; therefore, changes to the physical layer aspects should be done independent of attributes of the other layers of the OSI model.

Changing the frequencies used by IEEE 802.16 compliant products requires a cost-benefit analysis. The benefits of using lower frequencies are increased range and greater flexibility in non-line-of-sight environments. However, these changes mean the use of frequencies with smaller frequency bands. For example military VHF

systems such as SINCGARS operate in the 30 MHz to 80 MHz band for a bandwidth of 50 MHz compared to the Redline AN-50e, which currently operates in the 5.735 GHz to 5.865 GHz range with available bandwidth of 130 MHz.

b. Low Probability of Detection (LPD)/Low Probability of Interception

Though designing a system with low probability of detection and interception would decrease the throughput available, the benefits to the warfighter far exceed the costs. Frequency hopping (FH) and direct sequence spread spectrum (DSSS) are mature concepts that can be implemented to IEEE 802.16 products. Techniques to decrease the radio frequency (RF) signature for operators on the battlefield must be analyzed further.

2. Form Factor

The AN-50e devices here at the Naval Postgraduate School have been used in a variety of scenarios to date and the systems have held up well. They have been embarked in transit cases, transported in automobiles, airplanes, and sea vessels, and deployed in laboratory settings, in Thailand, in the hills of the California Central Coasts and currently in New Orleans, LA. Also, as described in Chapter IV, the Marine Corps has deployed these systems in the Iraqi desert. Despite the survivability demonstrated to date, the gear should be hardened in order to meet military specifications.

During this study the AN-50eFT manpack radio was made available by Redline for testing in the COASTS and TNT research experiments. This version of the AN-50 was designed to meet Military Standards 810 (Mil-Std 810) for rated enclosures and shows Redline Communications' ability to adapt the hardware to meet military applications. The radio came in olive drab as opposed to its typical grey, it used DC power from two Lithium batteries versus AC power, was splash-resistant, and had the T-58 Transmitter/Receiver (transceiver) bolted onto the back to make the complete system manpackable. This system came with a 9 dBi omni-directional antenna but could easily connect to any antenna via IF-cable.

The usability of these systems will increase greatly when chip manufacturers such as Intel, mass market IEEE 802.16 Application Specific Integrated Circuits (ASICs).

Chip manufacturers have begun to design these devices with the goal of making them commercially available in 2006. The introduction of these ASICs will bring IEEE 802.16 wireless links to mobile platforms such as laptop computers and personal digital assistants (PDAs).

Military program officers responsible for the acquisition of tomorrow's system who feel this technology can be leveraged by military communities should express their requirements to vendors capable of adapting COTS technology for military use.

3. Antenna Deployment and Alignment

High-gain, narrow-beam antenna systems require a significant investment in time and personnel to deploy. Within a military context, these types of antennas are typically elevated through the use of an antenna mast. One example is the OE-254, which is an antenna mast that raises the radiating element for the SINCGARS radio to a height of 42 feet. Though the alignment of high-gain antennas is time consuming, it is a requirement for optimal network connectivity. Therefore, the process and tools should be analyzed in order to offer greater ease of deployment to the military user.

The signaling feature of the T-58 transceiver is a move in the right direction, as it offers the user immediate audible feedback as to the quality of the wireless link. This device proves effective when the antenna is at a height that still allows the operator to adjust the antenna vertically and horizontally. The challenge is to perform precise antenna alignment when the antenna is 30 feet in the air. Ongoing developments in the design of smart antennas might address this capability. Smart antennas could provide the system with far greater received signal strength, as it will automatically adjust to find the best received signal.

4. Automate the Promotion of a Subscriber Station

Redundancy is a crucial aspect for military networks. In today's dynamic battlefield, communications systems can go offline due to exceeding line-of-sight, for maintenance or administrative reasons, and enemy activity. Given this environment, the BS could be a single point of failure.

Redundancy can be provided today in two ways. The first is by providing excess equipment. This is done by configuring two AN-50e devices as redundant BSs. Each is

configured to support all valid SSs and operate in parallel. The primary system is set to transmit at the power level required to support the wireless network and the alternate BS is configured to transmit at a very low level. SSs will detect and associate to the BS with the higher RSSI. If for any reason, the primary BS should go offline, the alternate is configured, powered, and ready to assume responsibility for the network.

The second means requires communications personnel to reconfigure an SS manually to operate as a BS. Several key requirements are necessary for this to work. First, the SS selected for promotion requires radio connectivity to every other SS. Those stations without it will be unable to associate and to join the network. Secondly, the SS selected for promotion needs to have BS software installed. Reconfiguration of the SS will take time, and during that period the network will be inoperable.

The first method for providing redundancy, which essentially is over-provisioning, is the preferable method of the two; however, many scenarios can be proposed where this could fail. One example is the case of a battalion headquarters that comes under enemy attack and its communications equipment is damaged. Under these conditions, the ability of a company's SS to promote itself to the role of BS is desirable. The possibility to automate this functionality should be explored and developed.

5. Information Assurance

As presented in Chapter IV of this thesis, wireless links within the Marine Corps require FIPS-140-2 equivalent protection for unclassified networks and Type 1 encryption for Secret networks. The IEEE 802.16 standard and WiMAX certified products currently do not meet those requirements. Future products should incorporate some of these features in order to support Information Assurance requirements.

Several systems are available today that can deliver this service to these devices. For example, Air Fortress and Cranite Systems have FIPS-140-2 devices that can be employed over IEEE 802.16 technologies. In order to provide secret networks, communications personnel employ inline network encryption (INE) such as Taclane-175 to bulk encrypt all data. Future iterations of WiMAX products should incorporate additional security features to guard against traffic analysis and denial of services attacks.

C. SUMMARY

The recommendations in this chapter are modifications that can be addressed immediately and are concepts that are well understood and have a well established precedent in the evolution of previous communication technologies. The modifications to the physical layer such as adding LPD and LPI functionality can be handled without disrupting the higher order layers of the OSI model.

Modifying the form factor and developing a better way to deploy and align antennas, such as using smart antennas, will make the gear more resilient and greatly reduce set up time, two components that are critical to small units. Both of these components must be addressed if these technologies are to be adopted by a larger percentage of military applications.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

1. Problem Statement

The communications assets used throughout the Marine Air Ground Task Force (MAGTF) today were designed to support voice traffic and to meet service and application specific requirements. These systems have evolved as technology advanced, but their underpinnings as voice assets limits their ability to internetwork. The specialization of these radios has created an environment of point-to-point combat radio networks that are highly inflexible.

Despite the burden of legacy radio systems, warfighting concepts such as network centric warfare and to a smaller extent distributed operations envision information superior beings with increased combat power. These "Hyper-Beings" [42] will use real-time information from networked sensors and will use collaborative systems to increase the tempo of decision makers across the battlefield from the fire team leader to the Joint Task Force (JTF) Commander. Hyper-Beings enabled with information superiority are capable of independent action, can strike deeper, faster, and with overwhelming combat power.

Therefore the challenge is to develop the network that will support network centric operations and will afford our forces greater lethality, increased survivability, and a greater degree of self-synchronization.

This is a time when technology is advancing rapidly, and advanced wireless technologies hold the promise of delivering the high bandwidth, highly perishable information to the disadvantaged user operating on the low bandwidth tactical Internet. The Joint Tactical Radio System (JTRS) is the program approved to move the services into the future; however, its development and release is off schedule.

Given the existing communications environment, the future of network centric warfare, and the proliferation of new technologies, this is an exciting time. The adoption of tomorrow's network requires analysis and rigorous testing of emerging systems. The intent of this research was exactly that–to analyze if 802.11b secure wireless local area

networks (SWLAN) and IEEE 802.16 radio wide area networking devices could be used as a communications path for the command and control (C2) applications the warfighter employs on the battlefield.

2. Networking Requirements

Network centric warfare will require a communications architecture that is routable, meaning that routers at the border of networks will interconnect users on a host of IP-enabled communications systems. These networks will allow for the delivery of multicast traffic and for the dynamic assignment of Quality of Service (QoS) to different users, applications, and systems. Lastly, these systems will employ management agents such as simple network management protocol (SNMP).

3. Findings

The systems tested in this study are standards-based and have wide adoption in the market. They meet the above stated networking requirements and could be leveraged for military applications. The tests performed during this research validate the usability of these systems for certain missions as is. The Marine Corps' adoption of Redline Communications AN-50e for the LSWAN program in Iraq is further evidence.

Certain commercial-off-the-shelf adaptations are required in order to port these systems into a military domain; however, none of the recommendations break the specifications of the standard.

B. FURTHER RESEARCH

The following section briefly describes areas that warrant additional research within this domain.

1. Mobility

Large deployment of these technologies is not feasible until an adaptation for mobile users is addressed. The IEEE 802.16 Task Group is currently working on the IEEE 802.16e amendment, which addresses mobility. IEEE 802.16-2004 provisioned service to fixed stations only. When the mobility concerns are addressed and components are produced, these products will better support military applications and should be analyzed for applicability and implementation.

The IEEE 802.16 workgroup is addressing mesh functionality, and the development of the technology has direct applicability to military communications network, which by definition are mobile networks. When this functionality is developed and becomes commercially available, a thorough analysis will determine its applicability to military networks.

2. Layer 1 and 2 Security Solutions

Further experimentation is required in order to determine the interoperability of IEEE 802.16 products and layer 1 and 2 encryption technologies. A "Defense-in-Depth" approach is required; therefore, an analysis of layer 1 and 2 encryption techniques should be performed. Layer 1 bulk encryption can be done with inline network encryption devices such as the Taclane-175 or the soon-to-be released SecNet-54. In addition to testing for interoperability among these technologies, the cost in terms of throughput should be identified.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Department of Defense. *DoD Report to Congress: Network Centric Warfare* [online] http://www.dod.mil/nii/NCW/ncw_exec_sum.pdf Last accessed on 14 September, 2005

[2] Department of Defense. *DoD Report to Congress: Network Centric Warfare* [online] http://www.dod.mil/nii/NCW/ncw_exec_sum.pdf Last accessed on 14 September, 2005

[3] Alberts, David et al, Network *Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series February 2000

[4] Talbot, David, *How Technology Failed in Iraq*, Technology Review.Com [online] http://www.technologyreview.com/articles/04/11/talbot1104.asp?p=1 last accessed 14 September 2005

[5] United States Marine corps, *A Concept for Distributed Operations*, [online] https://www.mccdc.usmc.mil/FeatureTopics/DO/A%20Concept%20for%20Distributed%20Operations%20-%20Final%20CMC%20signed%20co.pdf last accessed 14 September 2005

[6] Office of the Secretary of Defense, Network *Centric Warfare Creating a Decisive Warfighing Advantage* [online] www.oft.osd.mil/library/library_files/document_318_NCW_GateFold-Pages.pdf last accessed 14 September 2005

[7] United States Marine Corps, *FORCEnet Making Network Centric Warfare a Reality*, [online] https://hqdod.hqmc.usmc.mil/FORCEnet/USMC/285,9,Slide 9 last accessed 15 September 2005

[8] Admiral Clark, Vern, USN, *Sea Power 21 Projecting Decisive Joint Capabilities* [online] http://www.chinfo.navy.mil/navpalib/cno/proceedings.html last accessed 14 September 2005

[9] Sea Viking Division, Marine Corps Warfighting Laboratory, Marine Corps Combat Development Command, *Sea Viking 2006 Distributed Operations Seminar Wargame #1 Assessment Report* [online] www.mcwl.quantico.usmc.mil/SV/DO%20WG%201%20Assessment%20Rpt%2016%20Dec%2004.pdf last accessed 14 September 2005

[10] United States Marine Corps, *Marine Corps Warfighting Publications (MCWP) 6-22* [online] https://www.doctrine.usmc.mil/aspweb/magtf-ops.asp last accessed 14 September 2005

[11] Project Manager Communications Systems, Marine Corps Systems Command, *MAGTF C4ISR Communications Systems*, [online] http://www.marcorsyscom.usmc.mil/sites/pmcomm/index.asp last accessed 14 September 2005

[12] United States Marine Corps, *Marine Corps Reference Publications (MCPR) 3-40.3A* https://www.doctrine.usmc.mil/signpubs/r3403a.pdf last accessed 14 September 2005

[13] 3rd Marine Regiment Combat Standard Operating Procedures (SOP), *Chapter 10 Communications*, May 2003

[14] Television Equipment Associates, *Personal Role Radio* [online] http://www.swatheadsets.com/PRR/PRR_leaflet_web.pdf last accessed 14 September 2005

[15] DACT Program Officer, Marine Corps Systems Command, *D-DACT Operator's Handbook* Version 3.6.5.1

[16] Chisholm, Patrick, *Handheld Net-Centricity*, Military Information Technology Online, [online] http://www.military-information-technology.com/print_article.cfm?DocID=577 last accessed 14 September 2005

[17] Allbritton, Christopher, *Birth of a Toughbook* [online] http://www.popularmechanics.com/technology/computers/1279251.html Last accessed on 14 September 2005

[18] Joint Interoperability Test Command, *Intelligence Operations Server (IOS) Versions 1 & 2, Tactical Combat Operations/Intelligence Analysis System (TCO/IAS),* [online] http://jitc.fhu.disa.mil/gccsiop/interfaces/ios.htm last accessed 14 September 2005

[19] United States Marine Corps, *Command and Control Personal Computer*, Acquisitions Programs and Terms [online] http://hqinet001.hqmc.usmc.mil/p&r/concepts/2005/PDF/Ch3PDFs/CP05%20Ch3P1%20CEP%20pg%20143_Command%20and%20Control%20Personal%20Computer.pdf last accessed 14 September 2005

[20] Bergman, Ken. *Integration of Topographic Engineering Skills and Tools – Providing Assured Mobility With C2 Systems*, Engineer, [online] http://www.globalsecurity.org/military/library/report/2005/050100-bergman2.pdf last accessed 15 September 2005

[21] United States Marine Corps, *Marine Corps Information Assurance Operational Standard 014 Wireless Local Area Networks V1.0 15* February 2005

[22] United States Marine Corps, *Use of the Harris SecNet Secure Wireless Networking Products in the MCEN,* 30 September 2005

[23] Nordin, Brandon, *Certified Wireless Network Administrator (CWNA) Official Study Guide Third Edition*, McGraw Hill, 2005

[24] Durbano, Steven, Matkowski, Joe, *Secure Wireless Networking SecNet-11 Testing* CenGen, December 2002

[25] Tennesen, Andreas, *Ad-Hoc and OLSR*, [online] http://www.olsr.org/index.cgi?action=adhoc last accessed 14 September 2005

[26] Clausen, T., Jacquet, P. *Optimized Link State Routing Protocol (OLSR) Request for comments 3226* [online] http://ietf.org/rfc/rfc3626.txt last accessed 14 September 2005

[27] Durbano, Steven, *MANET Update,* CenGen, December 2004

[28] The IEEE 802.16 Working Group on Broadband Wireless Access Standards Website [online] http://www.ieee802.org/16/index.html last accessed 15 September 2005

[29] WiMAX Forum Website [online] http://www.wimaxforum.org/technology last accessed 15 September 2005

[30] Olexa, Ron, *Implementing 802.11b, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations.* Elsevier Inc, 2005

[31] Redline Communications Website. [online] http://www.redlinecommunications.com/index.html?products/an50/an-50_ptm.html last accessed 15 September 2005

[32] Redline Communications, *AN-50e PTP System User Manual*, March 2004

[33] Redline Communications, *AN-50e Field Terminal Mechanical Concept* PowerPoint Presentation December 2004

[34] Ixia Website [online] http://www.ixiacom.com/ last accessed 15 September 2005

[35] Ixia, *IxChariot Application Scripts Guide*, v.2004

[36] Logistics Modernization Team East, *LSWAN Brief II MEF 27 May 2005* [online] www.lejeune.usmc.mil/mclcat/Download.html last accessed 14 September 2005

[37] *MGEN the Multi-Generator Toolset* [online] http://mgen.pf.itd.nrl.navy.mil/ last accessed 15 September 2005

[38] *Installing Network Probe* [online] http://www.netadmintools.com/art231.html last accessed 15 September 2005

[39] Naval Postgraduate School, *COASTS Thailand Demon (May 2005) Concept of Operations*, May 2005

[40] Durbano, Steven, *MGEN TNT Results*, Electronic Mail 27 May 2005

[41] Durbano, Steven, *NetProbe TNT Results*, Electronic Mail 27 May 2005

[42] Markarian, Garik et al, IEEE 802.16.3c-01/33r2 "*OFDM Proposal for the IEEE 802.16a PHY Draft St*andard" [online] http://www.ieee802.org/16/tg3/contrib/802163c-01_33r2.pdf last accessed 15 September 2005

[43] Hayes-Roth, *Rick. Hyper-Beings: How Intelligent Organizations Attain Supremacy Through Information Superiority*, November 2003

BIBLIOGRAPHY

Boom, Derrick. *Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks*. Masters Thesis. Naval Postgraduate School. September 2004.

Garcia, Gilbert, Joseforsky, David. *Transformational Communications Architecture for the Unit Operations Center (UOC); Common Aviation Command and Control System (CAC2S); and Command and Control on-the-Move Network, Digital Over-the-Horizon Relay (CONDOR).* Masters Thesis. Naval Postgraduate School. June 2004.

Guice, Robert, Munoz, Raymond. *IEEE 802.16 Commercial Off the Shelf (COTS) Technologies as a Compliment to Ship to Objective Maneuver (STOM) Communications*. Masters Thesis. Naval Postgraduate School. September 2004.

Harris Corporation, *SecNet 11 Secure Wireless Local Area Network System User Guide,* June 2002.

IEEE Computer Society. *Achieving Wireless Broadband with WiMAX.* June 2004.

Intel Corporation. *Adaptive Modulation (QPSK, QAM).* White Paper [online] http://www.intel.com/netcomms/technologies/wimax/303788.pdf last accessed 15 September 2005

Intel Corporation. *Orthogonal Frequency Division Multiplexing.* White Paper [online] http://www.intel.com/netcomms/technologies/wimax/303787.pdf last accessed 15 September 2005

Intel Corporation. *Understanding Wi-Fi and WiMAX as Metro-Access Solutions.* White Paper [online] http://www.intel.com/business/bss/industry/government/wimaxandmeshwhitepaper.pdf last accessed 15 September 2005

Marvin, Christopher. *802.16 OFDM Rapidly Deployed Network for Near Real Time Collaboration of Expert Services in Maritime Security Operations*. Masters Thesis. Naval Postgraduate School. September 2005.

Wi-Fi Planet Website. ONLINE http://www.wi-fiplanet.com/wimax/article.php/3302381 last accessed 15 September 2005

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. USCG C2 CEN
   Portsmouth, Virginia

5. Director, Marine Corps Research Center,
   MCCDC, Code C40RC
   Quantico, Virginia

6. Director, Training and Education,
   MCCDC, Code C46
   Quantico, Virginia

7. Lee Roether
   MCTSSA Operations
   Camp Pendleton, CA

8. Dan Boger
   Naval Postgraduate School
   Monterey, California

9. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

10. Carl Oros
    Naval Postgraduate School
    Monterey, California